handarina estantetapo en berales los polas en la gladitarinetera la companya esta esta companya de la companya esta companya de la companya de

# TECHNATION

Isabelle Mondou Deputy Minister of Canadian Heritage Department of Canadian Heritage

September 25, 2021

# RE: Submission of TECHNATION to Canadian Heritage Regarding Online Harms Legislation

# Deputy Minister Mondou,

Thank you for the opportunity to provide input into this consultation. Across the Canadian technology sector and our membership, there is agreement on the need to address digital safety. Our industry is already demonstrating leadership in the space and wants to support the Canadian government in achieving its policy objectives, based on robust experience creating and deploying content moderation systems globally. The regulation of the internet is an incredibly complex challenge, and the government should work with the tech sector to ensure new policies maintain freedom of expressions, protect marginalized communities and preserve due process while ensuring an operationally feasible regulatory regime. This regime must also keep Canada's longstanding commitment to net neutrality at its core, thereby maintaining and preserving a free and open internet.

We strongly believe that tackling illegal content online is a serious issue that will have long-lasting impacts on the way Canadians use the internet. We are supportive of the government's efforts to find ways to protect Canadians online, however, we are concerned that some aspects of the current proposal may have unintended negative impacts on access to valuable information and services, privacy and freedom of expression, and the innovation economy.

While traditionally TECHNATION would welcome the opportunity to provide these comments to the Department of Heritage, we raised concerns with both your officials and those at the Privy Council of the timing of these consultations, which took place during the federal general election. Given the subject of the consultations and alignment with political parties' election platforms, we also disagree that this consultation should have continued with a "Caretaker" government. Once a new Cabinet Minister is sworn in, we will be happy to provide further input.

As well, we do have other concerns on the process of these consultations. We believe that the consultation documents lack sufficient technical and policy details for industry members to understand the impacts of the proposed changes, risks, benefits and provide meaningful, detailed comments. The 8 week consultation period, done over the summer and as mentioned above, during an election, does not allow this important issue to generate the attention it deserves.

#### **Commitment by our Members**

As our members continue to iterate and strengthen approaches to meet evolving challenges surrounding online behaviours, our sector is moving with urgency, purpose and commitment to develop and enforce a range of policy, procedural, and product changes to help people feel safe, welcome, and to control their experience online. We support smart regulation with a focus on working with governments to ensure that regulation of the digital industry is practical, effective, feasible to implement, inclusive, and keeps certain core democratic values intact while promoting tech innovation.

5090 Explorer Drive, Suite 510, Mississauga, Ontario L4W 4T9 | ph. 905-602-8345, fax 905-602-8346

# TECHNATION

Delivering the highest safety standards requires investment, something that our members are committed to and have a track record of undertaking. TECHNATION's members have demonstrated this long-standing commitment to digital safety, as well as a history of working closely with governments, industry and civil society to identify and remove illegal and harmful online content. Many of our members have supported the *Voluntary Principles to Combat Online Child Sexual Exploitation and Abuse*, and are members of the *Technology Coalition* and *WeProtect Global Alliance*. In addition, TECHNATION members Facebook, Google, Microsoft and Twitter are founding members of the *Global Internet Forum to Counter Terrorism* (*GIFCT*) which works to counter terrorism and violent extremism online.

#### **Principles-based Approach**

We encourage the Canadian government to take a principles-based approach to digital safety in order to achieve a safe, inclusive and open online environment. Principles that should be considered include:

- Platforms are good faith actors who operate responsibly and in accordance with local laws.
- Respect the Charter of Rights and Freedoms (expression and due process)
- Respect net neutrality and maintain an open internet.
- Draw a clear line between illegal and harmful content.
- Consideration of global privacy regimes and obligations, including Mutual Legal Assistance Treaties (MLATs).
- Ensure clarity and transparency while respecting user privacy.
- Strive for global interoperability and policy harmonization.
- · Policies should prioritize accuracy over speed in flagging and removing content.
- Recognize each platform and services are different and not conducive to a one-size fits all approach.

#### **Our Concerns**

While TECHNATION supports the intent of the government to enhance digital safety online, we are concerned with the current proposal and the potential impact it could have on freedom of expression and other fundamental human rights. Specifically, we recommend greater clarification and adjustment to address these main areas of concern:

- <u>The scope of services to be covered</u>: The Online Harms Proposal should focus only on the services that pose the greatest risk.
- <u>The scope of content to be covered</u>: The regulation of particular content, including the issuance of mandatory removal orders, should be limited to clearly defined categories of content that are illegal in Canada. Legal but potentially harmful content should remain subject to the content moderation procedures adopted by service providers, in accordance with their own terms of service and guidelines.
- <u>The obligations on service providers</u>: Service providers should not be required to proactively monitor user content, or report user data or content to law enforcement without proper judicial authorization or MLAT.

# TECHNATION

- <u>The availability of safe harbour protections</u>: Service providers should have intermediary liability immunity to allow them to carry out good-faith content moderation and other actions to enhance digital safety. Safe harbour protections should apply equally to actions taken to comply with law, as well as "good Samaritan" voluntary measures.
- <u>The powers delegated to the Digital Safety Commissioner</u>: Powers delegated to the Digital Safety Commissioner (the "Commissioner") should be scaled back to better recognize the potential human rights impacts of decisions taken under digital safety legislation, to place limits on inspection and order-making powers, and provide greater transparency and oversight by Parliament. The powers should also be reflective of global trade norms and agreements, such as the CUSMA, as it relates to algorithms and source code provisions.

In addition to the broad concerns noted above the consultation lacks specific technical and policy elements required to fully respond to the impact of the proposal in order to respond accordingly. There are considerable technical challenges to take into account and industry engagement needed prior to the introduction of any new rules or regulations to combat online harms. We are pleased to see that the Government of Canada has begun this process, but note the importance of a whole of government approach to this issue and that all-sectors of industry are engaged in a meaningful way.

TECHNATION can organize a series of roundtables to discuss the technical elements and policy options. We would welcome the opportunity to collaborate with the Government of Canada on these.

Thank you for the opportunity to submit this commentary.

Veria French

Nevin French Vice-President, Policy

#### About TECHNATION

TECHNATION is the authoritative national voice for Canada's \$230 billion information and communications technology (ICT) industry. Canada's 44,000 ICT firms directly and indirectly generate over 1.2 million jobs in Canada. The ICT industry in Canada also creates and supplies goods and services that contribute to a more productive, competitive, and innovative economy and society. Our membership ranges from large multinational platforms, to leading Canadian internet-service providers (ISP) to cutting edge domestic tech companies.

For over 60 years TECHNATION, formerly the Information Technology Association of Canada (ITAC), has been the industry-government nexus for technology prosperity in Canada. As a member-driven, not-for-profit, vendor-neutral TECHNATION unites Canada's technology sector, governments, and communities to enable technology prosperity from coast to coast. Our top ten largest companies collectively employ over 92,000 Canadians in every region of the country.

 From:
 Denis Balazuc

 To:
 ICN / DCI (PCH)

 Subject:
 Canada's Internet Censorship Plan

 Date:
 September 25, 2021 8:34:14 AM

I am writing about the consultation for censoring (let's call it what it really is) the Internet with unsound laws that haven't been thought of properly, are obviously misinformed and lack awareness in how the Internet works.

I urge anyone involved with those decisions to review their homework and stop trying to transform Canada into a surveillance country - we have enough examples around the world about where this leads in the long term. I did not immigrate to Canada to be have my speech gouged or my means of working limited by some arbitrary decision about what is "right" or "wrong" to say or write.

I actually do not understand how mature individuals in the 21th century can in good conscience try to reproduce a scheme that has already failed in many countries (the UK is an example) and is simply not possible to implement technically without leading to endless litigations and court challenges. Canada is already suffering of the monopoly of big TELCO companies that are literally ruining us with exorbitant prices and scandalous practices, please do not add censorship to this pathetic situation.

While I can no longer put my trust in our politicians for managing our digital environment, I still hope you will make the right choice and repel this horrendous plan. Please keep Canada free.

Très Cordialement Denis Balazuc

Dissummit common på en kimis o la (sv. avir lanaés à l'hilomitikan Distairent releasett overvant fo Distairent releasett overvant fo



31 août 2021

# Commentaires sur l'approche proposée par le gouvernement fédéral pour s'attaquer au contenu préjudiciable en ligne

par Marie-Claude Girard, au nom du Rassemblement pour la laïcité

Le Rassemblement pour la laïcité est un regroupement d'individus et d'organismes ayant en commun la promotion de la laïcité comme philosophie humaniste de pensée et comme régime juridique régissant les relations entre les citoyens du Québec et leurs institutions publiques.

Fondé en 2010, il s'est donné dès le départ l'objectif de favoriser la concertation entre les divers intervenants, groupes, organismes et associations partageant cet objectif de promotion de la laïcité.

### CONTEXTE

La présente répond à l'invitation du gouvernement de commenter l'approche proposée pour s'attaquer au contenu préjudiciable en ligne. Cette approche comprend un nouveau cadre législatif et réglementaire, avec des règles sur la manière dont les plateformes de médias sociaux et autres services en ligne doivent traiter les contenus préjudiciables. Le cadre défini :

- les entités qui devraient être visées par les nouvelles règles,
- les types de contenu préjudiciable qui devraient être régis,
- · les nouvelles règles et obligations pour les entités réglementées ; et
- deux nouveaux organismes de réglementation et un conseil consultatif pour administrer et superviser le nouveau cadre et faire respecter ses règles et obligations.

Cette approche se veut complémentaire au projet de loi C-36, déposé le 23 juin 2021, pour :

- permettre à la Commission canadienne des droits de la personne d'examiner les plaintes de propagande haineuse et conférer au Tribunal des droits de la personne le pouvoir de trancher ces plaintes;
- modifier le Code criminel afin d'ajouter une définition du mot « haine » pour les infractions de propagande haineuse prévues à l'article 319 et créer un engagement de ne pas troubler l'ordre public pour la propagande haineuse et les crimes haineux.

Ce projet de loi a cependant été abrogé par le déclenchement des élections fédérales le 16 août 2021. L'invitation à commenter l'approche proposée semble toutefois se poursuivre puisqu'elle apparaît toujours sur le site du ministère du Patrimoine canadien. Voici donc quelques commentaires et recommandations sur la partie de cette consultation concernant les contenus préjudiciables liés à la haine et à l'extrémisme en ligne.

#### ENJEUX

Deux enjeux majeurs préoccupent particulièrement le *Rassemblement pour la laïcité* dans le cadre de cette consultation à savoir la nécessité de protéger la liberté d'expression à l'égard des religions et l'exception religieuse sur la propagande haineuse contenue dans le Code criminel.

# 1. Critique des religions

Les débats entourant l'adoption de la motion M-103 en 2017 ont clairement démontrés qu'il y avait souvent confusion entre la critique des religions et l'expression de propos haineux envers un groupe désigné.<sup>1</sup>

### Texte de la motion<sup>2</sup>

Que, de l'avis de la Chambre, le gouvernement devrait :

a) reconnaître qu'il faille endiguer le climat de haine et de peur qui s'installe dans la population;

*b*) condamner l'islamophobie et toutes les formes de racisme et de discrimination religieuse systémiques et prendre acte de la pétition e-411 à la Chambre des communes, ainsi que des problèmes qu'elle a soulevés;

c) demander que le Comité permanent du patrimoine canadien entreprenne une étude sur la façon dont le gouvernement pourrait

(i) établir une approche pangouvernementale pour la réduction ou l'élimination du racisme et de la discrimination religieuse systémiques, dont l'islamophobie, au Canada, tout en assurant l'adoption de politiques fondées sur les faits, qui soient d'application globale et axées sur la communauté,

(ii) recueillir des données pour contextualiser les rapports sur les crimes haineux et pour évaluer les besoins des communautés touchées; le Comité

<sup>&</sup>lt;sup>1</sup> https://ici.radio-canada.ca/nouvelle/1024073/motion-m-103-adoptee-les-communes-condamnent-lislamophobie

<sup>&</sup>lt;sup>2</sup> https://www.noscommunes.ca/members/fr/88849/motions/8661986

devrait présenter ses conclusions et ses recommandations à la Chambre dans les 240 jours civils suivant l'adoption de la présente motion, pourvu que, dans son rapport, le Comité devrait formuler des recommandations que pourra appliquer le gouvernement afin de mettre davantage en valeur les droits et libertés garantis dans les lois constitutionnelles, y compris la Charte canadienne des droits et libertés.

En l'absence de définition concrète de « l'islamophobie », les opposants à la motion M-103 craignaient qu'elle constitue une limite excessive à la liberté d'expression en ce qui a trait à la critique légitime de l'islam, en plus d'associer cette critique à du racisme et à de la discrimination systémique. D'autres ont soulevé que la motion ne ciblait qu'une seule religion, donnant ainsi des privilèges à une religion ou à une communauté aux dépens des autres. Cet épisode tumultueux de l'histoire récente du parlement canadien démontre, hors de tout doute, l'importance de distinguer critique des religions et propos haineux envers un groupe désigné, afin de ne pas limiter indûment la liberté d'expression au Canada.

N'oublions pas que, comme le disait Sam Haroun en 2018, la liberté de religion passe par la liberté de critiquer la religion :

« Croire ou ne pas croire est l'acte libre d'un esprit libre. Cela veut dire deux choses : d'abord, tout individu est libre d'être athée, chrétien, juif, musulman ou hindouiste, et doit reconnaître à autrui le même droit ; ensuite, la foi religieuse et l'incroyance ne sont pas des absolus scellés dans l'infaillibilité, imperméables à toute critique. Au contraire, c'est l'honneur d'une religion de se soumettre au libre arbitre, au doute et au jugement de ses adeptes et des adeptes d'autres convictions. » <sup>3</sup>.

En faits, tous les systèmes de penser, que ce soit le capitalisme, le communisme, le fascisme, l'athéisme, le catholicisme, l'islam ou autre, doivent pouvoir être critiqués. C'est le choc des idées et des connaissances qui fait avancer une société. Par contre, l'encouragement au génocide et l'incitation publique à la haine contre un groupe identifiable, tel que défini par le Code criminel<sup>4</sup>, doivent bien sûr être proscrits.

2. Exception religieuse du Code criminel

Le Code criminel canadien sur la propagande haineuse comporte une « exception religieuse », soit l'alinéa 319(3)b).

#### Incitation publique à la haine<sup>5</sup>

<sup>&</sup>lt;sup>3</sup> <u>https://www.ledevoir.com/opinion/idees/520885/la-liberte-de-religion-passe-par-la-liberte-de-critiquer-la-religion</u>

<sup>&</sup>lt;sup>4</sup> 318(4) Au présent article, groupe identifiable s'entend de toute section du public qui se différencie des autres par la couleur, la race, la religion, l'origine nationale ou ethnique, l'âge, le sexe, l'orientation sexuelle, l'identité ou l'expression de genre ou la déficience mientale ou physique.

<sup>&</sup>lt;sup>5</sup> https://laws-lois.justice.gc.ca/fra/lois/C-46/section-319.html?wbdisable=true

**319 (1)** Quiconque, par la communication de déclarations en un endroit public, incite à la haine contre un groupe identifiable, lorsqu'une telle incitation est susceptible d'entraîner une violation de la paix, est coupable :

a) soit d'un acte criminel et passible d'un emprisonnement maximal de deux ans;

**b)** soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

### Fomenter volontairement la haine

(2) Quiconque, par la communication de déclarations autrement que dans une conversation privée, fomente volontairement la haine contre un groupe identifiable est coupable :

a) soit d'un acte criminel et passible d'un emprisonnement maximal de deux ans;

**b)** soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

# Défenses

(3) Nul ne peut être déclaré coupable d'une infraction prévue au paragraphe (2) dans les cas suivants :

a) il établit que les déclarations communiquées étaient vraies;

 b) il a, de bonne foi, exprimé une opinion sur un sujet religieux ou une opinion fondée sur un texte religieux auquel il croit, ou a tenté d'en établir le bien-fondé par argument;

(...)

Cette disposition relative à la propagande haineuse offre une protection au discours religieux portant préjudice à un groupe identifiable, s'il est prononcé de bonne foi et fondé sur un texte religieux. Rappelons que les textes de plusieurs des grandes religions comportent des propos qui dénigrent ou prônent la haine contre les apostats, les incroyants, les femmes, les homosexuels voire certains groupes ethniques ou raciaux. Certes, la majorité des croyants font assurément la part des choses et interprètent les textes religieux dans un contexte plus contemporain et respectueux de toutes et de tous. Mais d'autres en font une lecture rigoriste qui peut se traduire en un discours dégradant pour plusieurs citoyens.

Les discours haineux contenus dans des prêches, des conférences, des vidéos, des tweets ou autres, basés sur un texte religieux ou son interprétation, même lorsque prononcés de bonne foi, ne doivent plus être tolérés au Canada. Malheureusement, ces derniers existent. À titre d'exemple, pour n'en nommer que deux, le discours homophobe d'un pasteur de la Congrégation Régina Victory Church<sup>6</sup> en mars dernier ou encore les vidéos de deux imams montréalais dénoncés par le Centre consultatif des relations juives

<sup>\*</sup> https://ici.radio-canada.ca/nouvelle/1776230/homophobie-religion-pasteur-terry-murphy-sermon

et israéliennes (CIJA)<sup>7</sup> en 2017. Ces discours constituent, sans aucun doute, un frein au mieux vivre ensemble en société.

Une pétition a été déposée à la Chambre des communes en 2018<sup>8</sup> demandant l'abrogation de cet article, mais sans succès. Cette pétition faisait valoir, entre autres, que les textes de plusieurs des principales religions comportent des propos qui dénigrent et prônent la haine contre les incroyants, les femmes, les homosexuels ou certains groupes ethniques ou raciaux. La réponse donnée par l'honorable Jody Wilson-Raybould, ministre de la Justice et procureur général du Canada<sup>9</sup> pour justifier ce refus se basait sur une décision de la Cour Suprême<sup>10</sup> datant de 1990, soit précédant l'introduction de l'exception religieuse en 2004. Il est temps de rectifier la situation pour éliminer une exception qui n'a pas sa raison d'être si on veut sérieusement d'attaquer aux discours haineux en ligne.

Donc, oui au respect des religions, sauf lorsque cela s'inscrit en porte-à-faux avec le droit qu'ont les citoyens au respect et à la dignité humaine. L'exception religieuse relative à la Propagande haineuse doit être abrogée pour contrer le discours haineux au Canada. Il n'est pas suffisant de mieux définir le discours haineux et de proposer un nouveau cadre législatif et réglementaire pour les médias sociaux. Il faut agir sur ses causes.

RECOMMANDATIONS

Module 1 : Un nouveau cadre législatif et réglementaire pour les médias sociaux

La législation modifierait les définitions du droit existant pour les adapter à un contexte réglementaire plutôt que pénal et établirait une obligation légale pour les entités réglementées de prendre toutes les mesures raisonnables pour rendre les contenus préjudiciables inaccessibles au Canada. Le cadre réglementaire exigerait que les entités réglementées déclarent certains types de contenu aux forces de l'ordre et au *Service canadien du renseignement de sécurité* afin de permettre la mise en place d'enquêtes et de mesures de préventions appropriées. La loi proposée créerait également une nouvelle *Commission canadienne de sécurité numérique* afin de soutenir trois organismes qui mettraient en œuvre, superviseraient et appliqueraient le nouveau régime : le *Commissaire à la sécurité numérique du Canada*, le *Conseil de recours en matière numérique du Canada* et un *Comité consultatif d'experts*.

**Recommandation 1**:

Clairement indiquer, dans les mandats de la nouvelle *Commission canadienne de sécurité numérique* et des trois organismes sous sa supervision, que la critique légitime des religions ne fait pas partie des propos diffamatoires à traiter.

<sup>&</sup>lt;sup>7</sup> https://www.lapresse.ca/actualites/justice-et-faits-divers/actualites-judiciaires/201709/14/01-5133317-deux-imams-de-montreal-neseront-pas-accuses-de-discours-haineux.php

<sup>&</sup>lt;sup>8</sup> https://petitions.noscommunes.ca/fr/Petition/Details?Petition=e-763

<sup>&</sup>lt;sup>9</sup> https://www.ourcommons.ca/Content/ePetitions/Responses/421/e-763/421-02119 JUS F.pdf

<sup>10</sup> Décision R c Keegstra, 1990, 3 RCS 697.

Module 2 : Modifier le cadre juridique canadien

Ce module vise à compléter le projet de loi C-36 en proposant d'améliorer l'efficacité de la Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent un service Internet et de rationaliser le processus d'obtention de l'autorisation judiciaire d'acquérir les informations de base sur l'abonnée d'un acteur de menaces en ligne de la Loi sur le Service canadien du renseignement de sécurité.

Recommandation 2 :

Amender les modifications proposées dans le projet de loi C-36, visant à confier le mandat à la *Commission canadienne des droits de la personne* de traiter les plaintes de propagande haineuse, pour explicitement exclure la critique légitime des religions.

Recommandation 3 :

Abroger l'exception religieuse (alinéa 319(3)b)) du Code criminel canadien relatif à la Propagande haineuse.



Grassment commonsplit on series of the Lin and cample is Tallormation Discovery interest oversions to the Access Reministration Art



Submission of the Citizen Lab to the Federal Government's Proposed Approach to Address Harmful Content Online ("Online Harms Consultation")

Cynthia Khoo, Lex Gill, and Christopher Parsons (Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto)

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St Gatineau QC K1A 0S5

[delivered electronically]

25 September 2021

# About the Citizen Lab and the Authors

- The Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto ("Citizen Lab"), is an interdisciplinary laboratory which focuses on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.
- 2. For over a decade, the Citizen Lab has used a mixed methods approach that combines techniques from network measurement, information security, law, and the social sciences to research and document information controls—including Internet censorship and surveillance—that impact the openness and security of digital communications and pose threats to human rights. Our work has investigated digital espionage against civil society; documented Internet filtering and other technologies and practices that impact freedom of expression online; analyzed privacy, security, and information controls of popular applications; and examined corporate and state accountability, transparency, oversight, and control in relation to information technologies, including the impact of those technologies on historically marginalized groups.

At Trinity College 1 Devonshire Place Toronto, ON Canada M55 3K7 T: 416,946,8900 F: 416,946,8915 At the Observatory 315 Bloor Street West Toronto, ON Canada M55 0A7 1: 416,946,8929 F- 416,946,8877 minkschool utorento.ca

At the Canadiana Gallery 14 Queen's Park Crescent West Toronto, ON Canada M55 3K9 1: 416.978.5120 F- 416.978 5079



- 3. The Citizen Lab's groundbreaking research has resulted in over 120 publications and reports,<sup>1</sup> generated more than 25 front page exclusives in *The New York Times*, *Washington Post*, and other leading outlets, and received numerous international awards and recognitions. This scholarship has been cited by policymakers, academics, and civil society as foundational to the understanding of digital technologies, human rights, and global security.
- 4. The authors of this submission have diverse expertise in the freedom of expression, privacy, and/or equality rights implications of emerging technologies, including the specific kinds of technologies discussed in the "Technical Paper" associated with this consultation. We also have expertise in related areas of technology law and policy raised by this consultation, including adjacent questions of constitutional law, intermediary liability, privacy, national security, jurisdictional issues, and criminal evidence. We, alongside our colleagues at the Citizen Lab, have produced research on technologies closely related to this consultation, including consumer spyware apps ("stalkerware") and nation-state spyware, content filtering tools, anonymity tools, social media apps and platforms, and predictive policing and algorithmic surveillance technologies, among others. We have also published on issues related to corporate data collection, management, and disclosure and the relevant law and policy questions engaged by these issues. Each of us has routinely provided recommendations for technology, policy, and legal reform related to our respective findings in Canada and in various international fora.
- 5. We have reviewed the consultation materials, including the "Technical Paper" and the "Discussion Guide", associated with the government's proposal to address what it has referred to as "online harms".<sup>2</sup> We provide the following comments in response to that consultation process, divided into the following sections:
  - A. This Consultation Is Inadequate;
  - B. The Proposed Regime Will Not Achieve Its Intended Goals;
  - C. The Scope of the Proposal Is Overbroad and Incoherent;
  - D. Automated Enforcement Exacerbates Pre-Existing Problems;
  - E. Unidirectional Takedown Incentive Will Likely Be Inequitable and Unconstitutional;
  - F. Surveillance and Mandatory Reporting Requirements Are Dangerous and Chilling;
  - G. New CSIS Powers Are Unjustified and Inappropriately Included in this Consultation; and
  - H. Conclusion: Rewrite the Proposal from the Ground Up.

A complete list of the Citizen Lab's publications, including research reports, articles, book chapters, resources and external submissions to government and international bodies is available online: <a href="https://citizenlab.ca/publications/">https://citizenlab.ca/publications/</a>.

Болан на самой в Границијац 20 сапасти сећена во состате 1011 - 4 селет се отпесетот с

<sup>&</sup>lt;sup>2</sup> "Have your say: The Government's proposed approach to address harmful content online", Government of Canada (online): <a href="https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html">https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html</a>.



растительскими парто и заказе раз и на списти в Трібини на растительники селотер ин протесто селотельского ст

OF GLOBAL AFFAIRS & PUBLIC POLIC

# A. This Consultation Is Inadequate

- As a preliminary comment, the consultation process undertaken by the government on these proposals has been grossly inadequate.
- 7. The public materials, including the "Technical Paper", are vague, ambiguous, and in some cases contradictory. They fail to address some of the most obvious technical, legal, and constitutional problems they create—including problems that would negatively impact the purported "beneficiaries" of the proposed law. Some elements of the proposed measures are highly derivative of foreign legal regimes (including Germany's NetzDG regime and the United Kingdom's controversial Online Safety Bill), but lack the coherence or corresponding safeguards present in those schemes, and fail to respond to the criticism those regimes have faced on human rights grounds. Even the basic scope of what entities will be subject to the proposed measures is fundamentally uncertain because the definition of an "Online Communication Service Provider (OCSP)" is not sufficiently precise as presented,<sup>3</sup> and is subject to further change and indeterminacy through future regulations.
- 8. The materials also fail to offer any rational justification or evidence to demonstrate that the sweeping legal reforms proposed are likely to substantially mitigate the problems they purport to address. As a result, the materials lack a sufficient basis for comment and analysis, undermining the very function of a public consultation.
- 9. Though this consultation was preceded by a series of private, invite-only meetings between civil society groups and representatives from Heritage Canada and the Department of Justice, there is little to no evidence that the concerns raised by stakeholders at these meetings were accounted for in the government's proposal.<sup>4</sup> The government has been on notice that many of its proposals raise serious ethical, practical, and constitutional doubts since at least 2020, but these issues remain fundamentally unaddressed in the public materials. This failure to adjust course has undermined confidence among many experts and advocates that the function of the present consultation is, in fact, to consult, rather than to retroactively legitimize a series of foregone conclusions.
- 10. Finally, the period for written comments—particularly when limited to the end of summer during a federal election and global pandemic—has been insufficient to do justice to the sweeping proposals set out in the consultation materials. We would note that two of us are signatories to a public letter that

For example, the "Discussion Paper" specifies that the category of OCSP is meant to "exclude travel review websites", yet such websites would seem to fit within the proposed definition of providing an OCS, a service that "enable[s] users of the service to communicate with other users of the service, over the internet", and the "Technical Paper" does not provide an explicit basis for exceptions from this definition.

We would note that in December 2020, for example, two authors of this submission and a staff lawyer from another civil society organization met with Arif Virani (Parliamentary Secretary to the Minister of Justice and Attorney General of Canada) and Caroline Bourbonnière (Senior Advisor on Digital Policy to the Minister of Canadian Heritage) regarding this proposal. Many of the issues in this submission were flagged to the government's representatives at this time. One of the authors of this submission raised the same issues in speaking at a closed roundtable which also occurred in December 2020, where the Minister of Canadian Heritage Stephen Guilbeault was present, in addition to representatives of the same departments above.



protested the continuation of this consultation on the basis that it should not have proceeded after the government dissolved Parliament and called a federal election.<sup>5</sup> In our view, it was deeply inappropriate for this consultation to have continued during the caretaker period and we are disappointed that the government has failed to respond to these concerns.

# B. The Proposed Regime Will Not Achieve Its Intended Goals

- 11. Technology-facilitated violence, abuse, and harassment is a real problem. Whether the violence, abuse, and harassment is based on gender (collectively, "TFGBV"), race, sexual orientation, other characteristics protected in Canadian equality law, or—more often than not—an intersecting combination of multiple characteristics, it plagues members of historically marginalized groups, who are routinely silenced and driven off the Internet as a result. This issue is serious and pressing, and it deserves and requires urgent and sustained attention from governments, technology companies, scholars, and civil society at every level.
- 12. In the same vein, thoughtless legislative measures to address these same issues for reasons of political expediency, or with insufficient care, thoughtfulness, intersectional and equitable considerations, and while lacking understanding of the practical and sociotechnical implications of such measures when implemented, do a profound disservice to the issue—as well as to targets, victims, and survivors, and to those historically marginalized groups whom online abuse, including NCDII and hate speech, most devastates.
- 13. In this respect, the proposals advanced by the government fail to account for the scholarship, concerns, and experiences of underrepresented, historically marginalized, and vulnerable individuals and communities. These are, of course, the very people who face the vast majority of technology-facilitated abuse, harassment, and violence—including women; Black, Indigenous, or otherwise racialized individuals; LGBTIQ+ individuals; individuals with disabilities; members of religious, linguistic and ethnic minority communities; immigrants and refugees; survivors of sexual violence, racist violence, and hate crimes; and sex workers—as well as individuals whose identities overlap multiple intersections among those groups.<sup>6</sup>
- 14. Research—including research produced by the Citizen Lab—has consistently demonstrated that Internet filtering and content monitoring technologies often result in the disproportionate censorship and surveillance of historically marginalized individuals and communities.<sup>7</sup> The technical interventions

Болан на споста в Пайлания Фосналания собласти воссоватью ИК Населен астанательного со

See OpenMedia et al, "Open letter: Defer consultations on the Internet until after the election" (2021), online: <a href="https://openmedia.org/article/item/open-letter-requesting-rescheduling-of-open-internet-consultations-">https://openmedia.org/article/item/open-letter-requesting-rescheduling-of-open-internet-consultations-</a>.

See report and all sources cited within: Cynthia Khoo, "Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence" (2021), at 23-28, online (pdf): *Women's Legal Education and Action Fund (LEAF)* <a href="https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf">https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf</a>.

<sup>&</sup>lt;sup>T</sup> See e.g., Jakub Dalek, Nica Dumlao, Miles Kenyon, Irene Poetranto, Adam Senft, Caroline Wesley, Arturo Filastò, Maria Xynou, and Amie Bishop. "No Access: LGBTIQ Website Censorship in Six Countries" (August 2021), Citizen Lab Research Report No. 142, University of Toronto, online: <a href="https://citizenlab.ca/2021/08/no-access-lgbtiq-website-censorship-in-six-countries/">https://citizenlab.ca/2021/08/no-access-lgbtiq-website-censorship-in-six-countries/</a>; Jakub Dalek, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft,



proposed by the Canadian government in the context of this consultation are emblematic of such an approach. The consultation materials advance an aggressive, algorithmic, and punitive regime for content removal it proposes, without any substantive equality considerations or clear safeguards against abuse of process. They also demonstrate the government's willingness to enlist and empower law enforcement and intelligence agencies to intervene on these issues—whether or not the victim or survivor has consented to such intervention.

- 15. In our view, any proposal that advances a superficial conception of safety for disadvantaged groups at the expense of their freedom to speak, create, relate, and organize, represents a false and potentially exploitative (and unconstitutional) promise. Furthermore, these measures encroach on individuals' right to privacy in serious ways, without substantially increasing "safety" in any case. This approach is predicated on a deeply paternalistic view that reduces vulnerable individuals to their right to security—again, a right that will not even necessarily be enjoyed under the proposed measures—rather than respecting the full constellation of their human rights and political entitlements, including the right to full and equal participation in democratic life.
- 16. The proposals similarly fail to account for the importance of protecting the kinds of expression that are most central to a free and democratic society—including journalism, academic scholarship and public interest research, debate, artistic creation, criticism, and political dissent, particularly when engaged in by members of historically marginalized groups. While the consultation purports to narrowly target five categories of already-illegal content,<sup>8</sup> there is almost no doubt that the proposed measures will have collateral consequences on lawful, democratic, and equality-advancing expression, including initiatives to document human rights violations,<sup>9</sup> creative forms of advocacy and protest, content that normalizes and celebrates the full diversity of sexual expression,<sup>10</sup> and efforts to de-escalate and counter violently extreme and harmful expression.

Колана на селото в Поймателна Составал селото воссователо НЕ НЕСЕТЕ во протокото с

and Ron Deibert. "Planet Netsweeper" (April 2018), Citizen Lab Research Report No. 108, University of Toronto, online (pdf): <a href="https://tspace.library.utoronto.ca/bitstream/1807/95393/1/Report%23108--Planet%20Netsweeper.pdf">https://tspace.library.utoronto.ca/bitstream/1807/95393/1/Report%23108--Planet%20Netsweeper.pdf</a>; Ronald Deibert, Lex Gill, Tamir Israel, Chelsey Legge, Irene Poetranto, Amitpal Singh, "Submission to the UN Special Rapporteur on Violence Against Women, its Causes, and Consequences" (November 2017), online (pdf): *Citizen Lab* <a href="https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf">https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf</a>>.

Though even this is not, strictly speaking, accurate, as the definitions proposed would likely encompass certain forms of content which is currently unambiguously lawful, and the definitions of key terms are subject to change through regulation.

<sup>&</sup>lt;sup>9</sup> See e.g., Hadi Al Khatib & Dia Kayyali, "YouTube Is Erasing History", New York Times (23 October 2019), online: <https://www.nytimes.com/2019/10/23/opinion/syria-youtube-content-moderation.html>; and Belkis Wille, "'Video Unavailable': Social Media Platforms Remove Evidence of War Crimes" (September 2020), online: Human Rights Watch <https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes>.

<sup>&</sup>lt;sup>10</sup> See e.g., Cynthia Khoo, "Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence" (2021), at 138-39, online (pdf): *Women's Legal Education and Action Fund (LEAF)* <a href="https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf">https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf</a>.



#### Раздиональская на парто со закале. Коластика са 2010 година са с Фассаниа Саластика досто са се со се с Паттика се со Паттика се со с Паттика се со с Паттика се со с Паттика се со с Паттика се со се со

OF GLOBAL AFFAIRS & PUBLIC POLICY

# C. The Scope of the Proposal Is Overbroad and Incoherent

- 17. The five categories of content identified by the government include "terrorist" content; content that incites violence; hate speech; non-consensual distribution of intimate images (NCDII); and child sexual exploitation content. These categories have little in common, beyond the fact they are illegal, and even then, the relevant legal analysis and basis for illegality is completely unique to each. In truth, the categories are united by almost nothing—constitutionally, factually, practically, or ethically—other than the proposed remedy of content removal.
- 18. In our view, any legislative scheme that purports to unite all of these disparate kinds of content under a single framework is incoherent, counterproductive, and constitutionally untenable. Each of these types of content implicates different *Charter* rights, operational considerations, risks of collateral harm from overbroad removal (as well as different risks of harm from under-removal), and different public policy concerns militating in favour of and against government intervention. The *Charter* and Canada's international human rights obligations require the government to engage in a proportionality analysis when restricting expression—weighing it against the nature and gravity of the harm that results, including the impact on other *Charter* rights such as the right to equality, as well as the government's legitimate interest in mitigating that harm. This analysis is, by design, extremely contextual.
- 19. Certain kinds of content addressed by the consultation present a strong constitutional foundation for expeditious removal powers, assuming appropriate safeguards are in place. NCDII is perhaps the clearest example, because the expressive value in such content is marginal and its categorization relies on an essentially straightforward analysis of whether or not the imagery was distributed with consent. But other forms of content require a much more nuanced evaluation. In particular, speech which appears to approach the statutory definitions of "terrorist" speech, incitement to violence, or hate propaganda is much more likely to intersect with legitimate acts of artistic expression, satire, irony, critique, parody, or in-group reappropriation of discriminatory words and imagery—all of which are entitled to constitutional protection.
- 20. Furthermore, it is essential to note that Canada's criminal law provisions regarding "terrorist speech" are constitutionally weak and largely untested.<sup>11</sup> For years, civil society organizations have raised the concern that these provisions—creatures of former Bill C-51, and later Bill C-59—have or could be used in a manner that exacerbates the wrongful criminalization and surveillance of Muslim and Arab individuals in particular.<sup>12</sup>
- 21. In our view, any future legislative scheme must be designed and justified in relation to *specific* harms and on the basis of *specific* government objectives rather than in relation to a generalized remedy. The

<sup>&</sup>lt;sup>11</sup> For a more thorough discussion regarding the complexities of regulating "terrorist" content online and the constitutional vulnerabilities of the legislation currently in place, see Kent Roach, "Terrorist Speech under Bills C-51 and C-59 and the Othman Hamdan Case: The Continued Incoherence of Canada's Approach" (2019) 57:1 Alberta Law Review 203.

<sup>&</sup>lt;sup>12</sup> See Part F ("Surveillance and Mandatory Reporting Requirements Are Dangerous and Chilling") below for elaboration on this point.



remedial powers associated with these schemes should then be vested within administrative tribunals and courts that have the capacity—or that are given the funding and resources to build capacity—and subject-matter expertise to properly weigh the issues at stake. Newly created "one-size-fits all" administrative bodies are an inappropriate forum to account for the complex and disparate concerns raised herein.<sup>13</sup>

# D. Automated Enforcement Exacerbates Pre-Existing Problems

- 22. The consultation materials seem to encourage, if not all but mandate, the use of machine learning and similar automated technologies to enforce any legislated content regulations across OCSPs.<sup>14</sup> This drive towards automated enforcement may be rooted in the same rationale behind the government's decision to focus on the five types of content in question: a view that these categories are already relatively stable and narrowly circumscribed in Canadian law. To the extent that this is true in the law, the same cannot be said for these terms as they are likely to be interpreted or enforced by technology companies under the government's proposed approach—let alone through automated content moderation tools.
- 23. Before discussing the shortcomings of automated content moderation, it is worth establishing why human content moderation also poses difficulties. While courts, and to some degree expert administrative decision-makers, have generally proven capable of weighing context-sensitive and legal considerations on a case-by-case basis, the scale of the enforcement and removal envisioned by the consultation documents likely cannot, and will not, be achieved by human moderators.
- 24. Human reviewers of flagged content on social media are notoriously prone to error, due to factors such as problematic or misinterpreted company policies,<sup>15</sup> insufficient training, lack of time to properly assess content (as little as a matter of seconds), high-pressure environments that impose unimaginable stress, and lack of understanding of the content's cultural, social, or political context.<sup>16</sup> The reliance on human moderators across the digital platform industry is itself fraught; riddled with poor and

Колан на споста в Поблатила Себентали собласти воссовать с НЕ Череза поставляться — с

<sup>&</sup>lt;sup>13</sup> That being said, one of the authors of this submission has advocated in other work the creation of a specialized expert administrative body that would focus solely on technology-facilitated violence, abuse, and harassment against members of historically marginalized groups, for similar reasons of these issues requiring sensitive and nuanced treatment given their complexity and the vulnerability of impacted individuals. We emphasize that this recommendation likewise explicitly rejects the "one-size-fits-all" approach proposed in the consultation materials. See Cynthia Khoo, "Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence" (2021), at 225-27, online (pdf): *Women's Legal Education and Action Fund (LEAF)* <a href="https://www.leaf.ca/wpcontent/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf>">https://www.leaf.ca/wpcontent/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf>">https://www.leaf.ca/wp-</a>

<sup>&</sup>lt;sup>14</sup> "Technical Paper", at para 10.

See e.g., Julia Angwin & Hannes Grassegger, "Facebook's Secret Censorship Rules Protect White Men From Hate Speech But Not Black Children", *ProPublica* (28 June 2017), online: <a href="https://www.propublica.org/article/facebook-hate-speech-censorship-internal-documents-algorithms">https://www.propublica.org/article/facebook-hate-speech-censorship-internal-documents-algorithms</a>; and Samuel Gibbs, "Facebook bans women for posting 'men are scum' after harassment scandals", *Guardian* (5 December 2017), online: <a href="https://www.theguardian.com/technology/2017/dec/05/facebook-bans-women-posting-men-are-scum-harassment-scandals-comedian-marcia-belsky-abuse>">https://www.theguardian.com/technology/2017/dec/05/facebook-bans-women-posting-men-are-scum-harassment-scandals-comedian-marcia-belsky-abuse>">https://www.theguardian.com/technology/2017/dec/05/facebook-bans-women-posting-men-are-scum-harassment-scandals-comedian-marcia-belsky-abuse>">https://www.theguardian.com/technology/2017/dec/05/facebook-bans-women-posting-men-are-scum-harassment-scandals-comedian-marcia-belsky-abuse>">https://www.theguardian.com/technology/2017/dec/05/facebook-bans-women-posting-men-are-scum-harassment-scandals-comedian-marcia-belsky-abuse>">https://www.theguardian.com/technology/2017/dec/05/facebook-bans-women-posting-men-are-scum-harassment-scandals-comedian-marcia-belsky-abuse>">https://www.theguardian.com/technology/2017/dec/05/facebook-bans-women-posting-men-are-scum-harassment-scandals-comedian-marcia-belsky-abuse>">https://www.theguardian-marcia-belsky-abuse>">https://www.theguardian-marcia-belsky-abuse>">https://www.theguardian-marcia-belsky-abuse>">https://www.theguardian-marcia-belsky-abuse>">https://www.theguardian-marcia-belsky-abuse>">https://www.theguardian-marcia-belsky-abuse>">https://www.theguardian-marcia-belsky-abuse>">https://www.theguardian-marcia-belsky-abuse>">https://www.theguardian-marcia-belsky-abuse>">https://www.theguardian-marcia-belsky-abuse>">https://www.thttps://www.theguardian-marcia-belsky-abus

<sup>&</sup>lt;sup>16</sup> See e.g., Kate Klonick, "Facebook Under Pressure", *Slate* (12 September 2016), online: <a href="https://slate.com/technology/2016/09/facebook-erred-by-taking-down-the-napalm-girl-photo-what-happens-next.html">https://slate.com/technology/2016/09/facebook-erred-by-taking-down-the-napalm-girl-photo-what-happens-next.html</a>.



degrading working conditions; and characterized by low pay, professional insecurity, and psychological trauma.<sup>17</sup> Human content moderation on the scale required by the largest digital platforms raises serious issues of labour exploitation both in the home jurisdictions of major technology companies and internationally where such work is outsourced to third-party contractors in other countries.<sup>18</sup>

- 25. At the same time, automated content moderation such as through the deployment of machine learning algorithms fare little better. Examples abound of algorithmic errors in the content moderation field. They range from the superficially amusing, such as mistaking a photo of onions or of desert sand dunes for nudity,<sup>19</sup> to the politically disenfranchising—such as the algorithmic censorship of content by racial justice activists, adult content creators, sex education providers, documentors of war crimes and human rights violations, and political dissidents in authoritarian regimes.<sup>20</sup>
- 26. Further, algorithmic content moderation faces the same problems that inhere to nearly all forms of algorithmic decision-making, particularly in complex, contextual, socio-political environments. This includes the well-known issue of algorithmic bias—in particular, algorithmic bias against Black, Indigenous, and other racialized individuals and groups,<sup>21</sup> and gendered bias against women (both cis-

<sup>19</sup> Coby Zucker, "Nudity algorithm wrongly blocked company's onion images, Facebook admits, says adverts will be restored", National Post (7 October 2020), online: <a href="https://nationalpost.com/news/overtly-sexualized-st-johns-companys-onions-yes-onions-flagged-by-facebooks-nudity-algorithm">https://nationalpost.com/news/overtly-sexualized-st-johns-companys-onions-yes-onions-flagged-by-facebooks-nudity-algorithm</a>; and Melanie Ehrenkranz, "British Cops Want to Use AI to Spot Porn—But It Keeps Mistaking Desert Pics for Nudes", *Gizmodo* (18 December 2017), online: <a href="https://gizmodo.com/british-cops-want-to-use-ai-to-spot-porn-but-it-keeps-m-1821384511">https://gizmodo.com/british-cops-want-to-use-ai-to-spot-porn-but-it-keeps-m-1821384511</a>>.

See e.g., Danielle Blunt, Emily Coombes, Shanelle Mullin & Ariel Wolf, "Posting Into the Void" (2020), online: *Hacking//Hustling* <https://hackinghustling.org/wp-content/uploads/2020/09/Posting-Into-the-Void.pdf>; Shirin Ghaffary, "How TikTok's hate speech detection tool set off a debate about racial bias on the app", *Vox* (7 July 2021), online: <https://www.vox.com/recode/2021/7/7/22566017/tiktok-black-creators-ziggi-tyler-debate-about-black-livesmatter-racial-bias-social-media>; and Adam Smith, "Instagram Boss Says It Will Change Algorithm to Stop Mistreatment of Black Users, Alongside Other Updates", *Independent* (16 June 2020), online: <https://www.independent.co.uk/life-style/gadgets-and-tech/news/instagram-black-lives-matter-racism-harassmentbias-algorithm-a9567946.html>; Hadi Al Khatib & Dia Kayyali, "YouTube Is Erasing History", *New York Times* (23 October 2019), online: <https://www.nytimes.com/2019/10/23/opinion/syria-youtube-content-moderation.html>; Belkis Wille, "'Video Unavailable': Social Media Platforms Remove Evidence of War Crimes" (September 2020), online: *Human Rights Watch* <https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-warcrimes>; and Cynthia Khoo, "Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence" (2021), at 138-39, online (pdf): *Women's Legal Education and Action Fund (LEAF)* <https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf>.

<sup>21</sup> The Citizen Lab has closely examined algorithmic bias in the context of algorithmic decision-making tools used to assess immigration and refugee applications, and to inform policing decisions and other parts of the criminal justice system. See Petra Molnar & Lex Gill, "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System" (2018), online: *International Human Rights Program and the Citizen Lab* <https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf>; and Kate Robertson, Cynthia Khoo & Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in

Болан ала санова в Гранински Босаника) узбикана возгологиство На мерект астанаталиска со

<sup>&</sup>lt;sup>17</sup> See e.g., Sarah Emerson, "'A Permanent Nightmare': Pinterest Moderators Fight to Keep Horrifying Content Off the Platform", *OneZero* (28 July 2020), online: <a href="https://onezero.medium.com/a-permanent-nightmare-pinterest-moderators-fight-to-keep-horrifying-content-off-the-platform-4d8e7ec822fe">https://onezero.medium.com/a-permanent-nightmare-pinterestmoderators-fight-to-keep-horrifying-content-off-the-platform-4d8e7ec822fe</a>.

<sup>&</sup>lt;sup>18</sup> See generally Sarah T Roberts, Behind the Screen: Content Moderation in the Shadows of Social Media (New Haven and London: Yale University Press, 2019); and Elizabeth Dwoskin, Jeanne Whalen & Regine Cabato, "Content moderators at YouTube, Facebook and Twitter see the worst of the web—and suffer silently", Washington Post (25 July 2019), online: <https://www.washingtonpost.com/technology/2019/07/25/social-media-companies-are-outsourcing-their-dirtywork-philippines-generation-workers-is-paying-price/>.



and trans-), non-binary individuals, and members of the LGBTIQ+ community.<sup>22</sup> Studies have shown that "hate speech detection" algorithms often demonstrate anti-Black racial bias,<sup>23</sup> and YouTube has gained a reputation for systematically hiding, demonetizing, or otherwise undermining LGBTIQ+ content on its platform.<sup>24</sup>

27. These difficulties are only exacerbated by the fact that people in Canada speak and access content in hundreds of different languages and distinct dialects, not all of which receive the same degree of resources or attention from technology platforms, but all of which would be subject to the government's proposed content removal regime.

# E. Unidirectional Takedown Incentive Will Likely Be Inequitable and Unconstitutional

- 28. The incentive structure proposed by the government relies on large fines and other sanctions against technology companies to function. Combined with the 24-hour removal deadline, it is critical to note that the obligation and liability set out in the consultation materials appears largely unidirectional. The framework thereby rewards over-enforcement, with no countervailing forces to incentivize retention of content perceived as risqué or deviant by normative standards, but which remain legal, democratic, and often equality-advancing. This approach favours aggressive removal, the identification of false positives, and a risk-averse approach to sensitive or controversial content, as demonstrated by the empirical literature.<sup>25</sup> As emphasized above, it is the purported beneficiary groups of the proposed legislation—members of historically marginalized communities who are already silenced by both other users and the platforms themselves—who would disproportionately bear the brunt of wrongful takedowns. In our view, it is difficult to see how such an approach could be either equitable or constitutionally justifiable in Canada.
- 29. Moreover, 24 hours may be both too long *and* too short a window in which to require a platform company to act, depending on the type of content in question. The proposed legislation thus combines

Колан на спост в Пойнотории Фосновали собласт воссовать в ИК Малерии полотории со

Canada" (2020), online: Citizen Lab and International Human Rights Program <a href="https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf">https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf</a>.

Ari Ezra Waldman, "Disorderly Content" (17 August 2021) available at: <https://papers.ssrn.com/sol3/papers. cfm?abstract\_id=3906001>; and Daninel Leufer, "Computers are binary, people are not: how AI systems undermine LGBTQ identity" (6 April 2021), online: Access Now <https://www.accessnow.org/how-ai-systems-undermine-lgbtqidentity>.

<sup>&</sup>lt;sup>23</sup> Maarten Sap et al, "The Risk of Racial Bias in Hate Speech Detection" in Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics (Florence: Association for Computational Linguistics, 2019) 1668 at 1668. See also Charlotte Jee, "Google's algorithm for detecting hate speech is racially biased" (13 August 2019), online: *MIT Technology Review* <a href="https://www.technologyreview.com/2019/08/13/133757/googles-algorithm-for-detecting-hate-speech-looksracially-biased">https://www.technologyreview.com/2019/08/13/133757/googles-algorithm-for-detecting-hatespeech-looksracially-biased>.</a>

See e.g., Aja Romano, "A group of YouTubers is trying to prove the site systematically demonetizes queer content", Vox (10 October 2019), online: <a href="https://www.vox.com/culture/2019/10/10/20893258/youtube-lgbtq-censorship-demonetization-nerd-city-algorithm-report">https://www.vox.com/culture/2019/10/10/20893258/youtube-lgbtq-censorshipdemonetization-nerd-city-algorithm-report</a>.

<sup>&</sup>lt;sup>25</sup> See Daphne Keller, "Empirical Evidence of Over-Removal by Internet Companies Under Intermediary Liability Laws: An Updated List" (8 February 2021), online: *Center for Internet and Society (Stanford Law)* <a href="https://cyberlaw.stanford.edu/blog/2021/02/empirical-evidence-over-removal-internet-companies-underintermediary-liability-laws>.</a>



the worst of all worlds—potentially providing too little, too late in the case of NCDII, while courting unconstitutional overreach in the case of potential "hate speech" and "terrorist content". TFGBV experts consistently emphasize that speed is of the essence in the case of NCDII, given the danger in, devastating consequences of, and ease of downloading, reproducing, and further distributing the image or video, leading to further and repeated revictimization of the person depicted.<sup>26</sup> As mentioned above, identifying when something is NCDII (or child sexual exploitation) also poses fewer challenges compared to, in contrast, the likely more careful and nuanced analysis required for some situations of potential hate speech or "terrorist" content, for example.

30. Indeed, even Germany's NetzDG system, which has been deemed one of the more demanding platform regulation regimes, allows for up to seven days to assess and remove content that is not "manifestly unlawful".<sup>27</sup> Even to the extent that "hate speech" and "terrorist content" are unlawful, which has been the government's justification for their selection, it is far from the case that any given piece of content will manifestly fall within or outside of the relevant legal definitions. This is yet another instance demonstrating the incoherence, impracticality, constitutional fragility, and danger of addressing five legally, substantively, and sociopolitically different categories of content within the single blunt legal regime proposed. Addressing any of these issues in good faith requires separate, targeted legal regimes tailored to each category of content.

# F. Surveillance and Mandatory Reporting Requirements Are Dangerous and Chilling

- 31. It is essential to understand that at a technical level, any requirement to proactively filter or proactively remove harmful content (i.e., in the absence of complaints) necessarily imposes obligations on platforms or internet service providers to engage in proactive monitoring of their users' content. In other words, platform liability regimes such as those proposed in the consultation materials may not only lead to corporate and proxy censorship, but may also amount to implementing platform-wide (or internet-wide) surveillance systems of user expression. The rights to privacy, equality, and freedom of expression are intertwined and thus interdependently threatened by the proposed regime in this respect.
- 32. In that light, the fact that the government's proposals would explicitly deputize technology companies in the surveillance and policing of their users on behalf of Canadian law enforcement and intelligence agencies is all the more disturbing. The proposed requirement on service providers to "take all reasonable measures, which can include the use of automated systems, to identify harmful content that is communicated on its OCS and that is accessible to persons in Canada, and to make that harmful content inaccessible to persons in Canada" appears to be nothing short of a positive legal obligation to

Колан на селота в Поблатила Составал селота воссовать с НЕ Черета селотаталова — с

<sup>&</sup>lt;sup>26</sup> See e.g., Nicola Henry & Asher Flynn, "Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support" (2019) 25:16 Violence Against Women 1932 at 1933; and Emily Laidlaw & Hilary Young, "Creating a Revenge Porn Tort for Canada" (2020) 96 Supreme Court Law Review 147 at 165.

<sup>&</sup>lt;sup>27</sup> Heidi Tworek and Paddy Leerssen, "An Analysis of Germany's NetzDG Law" (15 April 2019) at 2, online (pdf): Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression <https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/2020/06/NetzDG\_TWG\_Tworek\_April\_2019.pdf>.



monitor users and moderate their content. This approach will inevitably result in disproportionate levels of user censorship, including foreign users abroad with no relationship to Canada.<sup>28</sup>

- 33. Further, we are deeply concerned with the mandatory reporting requirements proposed in the consultation materials. The "Technical Paper" proposes to require that technology companies retain detailed records about their users, as well as report specific kinds of user activity directly to the RCMP and/or other law enforcement agencies. It also contemplates mandatory reporting of certain kinds of content to the Canadian Security Intelligence Service (CSIS). Specifically, the government proposes that "an OCSP shall report information respecting terrorist content and content that incites violence that will be made inaccessible in accordance with this legislation".<sup>29</sup> Though this section of the consultation materials has been drafted in opaque language and provides broad, discretionary powers to Cabinet, it is clear that an automated mass informant scheme is what has ultimately been contemplated. These corporate informants, however, are essentially inescapable, given that they now play an almost infrastructural role in the social, relational, and political lives of people throughout Canada and around the world.
- 34. To this end, this proposal risks exacerbating the unconstitutional and discriminatory treatment of individuals whose information has been reported to law enforcement and/or CSIS. The reality is that these individuals are likely to belong to communities that are already disproportionately subjected to discriminatory over-criminalization by the police<sup>30</sup> and may be unjustly targeted for reporting to law enforcement. Such targeting and discriminatory treatment may be due to problematic or poorly applied platform policies, biased content moderation algorithms, or exploitation of the system by abusive users purposely targeting historically marginalized groups to drive them off a platform.<sup>31</sup>
- 35. We find it additionally troubling that how the government defines "terrorist content" varies throughout the consultation document, including the vague and recursive definition, "content that actively enourages terrorism and which is likely to result in terrorism".<sup>32</sup> (Indeed, definitional issues are a recurring problem throughout the "Technical Paper" as a whole.) A loose or unclear definition of "terrorist content" raises particular issues regarding potential consequences on the rights of Indigenous peoples to express their views online and to organize protests or demonstrations, in the context of Indigneous land and water rights, Indigenous self-determination, the fraught issue of Canadian sovereignty, and the appropriation of Indigenous lands for resource extraction projects,

<https://www.cigionline.org/static/documents/documents/SaferInternet\_Paper%20no%201\_0.pdf>.

Болан на спола в Пайлания Басалия страна в Страния Басалия социка в социка в социка На марахия в социка пола

<sup>&</sup>lt;sup>28</sup> The jurisdictional issues raised by this consultation are beyond the scope of our comments here, but we wish to acknowledge that they are both extensive and complex.

<sup>&</sup>lt;sup>29</sup> "Technical Paper", at para 22.

<sup>&</sup>lt;sup>30</sup> See e.g., Kate Robertson, Cynthia Khoo & Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (2020), at 15-18, online: *Citizen Lab and International Human Rights Program* <a href="https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf">https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf</a>.

<sup>&</sup>lt;sup>31</sup> See e.g., Suzie Dunn, "Technology-Facilitated Gender-Based Violence: An Overview" (2020), at 8, online (pdf): *Centre for* International Governance Innovation

<sup>&</sup>lt;sup>32</sup> "Technical Paper", at para 8.



Procession consistenti and an anna a la constante consistenti al Pathatana de 2000 micro constanta a constanta de 100 - Accession de constanta a moste constanta de 100 - Accessión de constanta a moste constanta de 100 - Accessión de constanta a moste constanta de 100 - Accessión de constanta a moste constanta de 100 - Accessión de constanta a moste constanta de 100 - Accessión de constanta de la moste constanta de 100 - Accessión de constanta de la moste constanta de 100 - Accessión de constanta de la moste constanta de 100 - Accessión de la moste constanta de la moste constanta de 100 - Accessión de la moste constanta de la moste constanta de 100 - Accessión de la moste constanta de la moste constanta de 100 - Accessión de la moste constanta de 100 - Accessión de la moste constanta de 100 - Accessión de 100 - Accessió

OF GLOBAL AFFAIRS & PUBLIC POLICY

given similar concerns that many raised in response to earlier iterations of proposed national security legislation, Bill C-51 and Bill C-59.<sup>33</sup>

- 36. Perhaps most saliently, given the purported objectives of the proposed legislation, mandatory reporting requirements and automated involvement of law enforcement and intelligence agencies will, again, disproportionately harm and abrogate the fundamental rights and freedoms of historically marginalized groups. The proposed measures will result in widely chilling effects on such individuals' online activities and *dissuade* victims or survivors from seeking assistance if they believe that law enforcement may become involved—particularly when engaged without consent and outside of the impacted person's control.
- 37. At the heart of these concerns is the fact that the very groups who are systematically targeted for online abuse, and who are frequently the subjects of both actual and perceived hate speech, are the exact same groups who have been historically victimized or re-victimized and discriminated against by Canadian law enforcement and intelligence agencies.
- 38. For example, systemic discrimination and state violence against Black, Indigenous, and otherwise racialized people, by law enforcement and at all levels of the criminal justice system, has been thoroughly documented by impacted individuals, racial justice experts and advocates, human rights lawyers and researchers, the government itself at all levels, and multiple commissions, inquiries, and investigations over the course of decades.<sup>34</sup> On another front, national security and intelligence activities have been closely tied to Islamophobia and racial profiling against Arab and Muslim individuals, or those who are perceived to be Arab or Muslim, resulting in incursions on their ability to exercise constitutional rights and freedoms, including online.<sup>35</sup>

<sup>&</sup>lt;sup>33</sup> See e.g., Doug Cuthand, "Bill C-51 has potential to scoop up aboriginal rights activists", *CBC* (6 May 2015), online: <https://www.cbc.ca/news/indigenous/bill-c-51-has-potential-to-scoop-up-aboriginal-rights-activists-1.3009664>; Hilary Beaumont, "The activists sabotaging railways in solidarity with Indigenous people", *Guardian* (29 July 2021), online: <https://www.theguardian.com/environment/2021/jul/29/activists-sabotaging-railways-indigenous-people>; Canadian Civil Liberties Association, "Submission to the Standing Committee on Public Safety and National Security regarding Bill C-59, *An Act respecting national security matters*" (January 18) at 14, online (pdf): *Canadian Civil Liberties Association* <https://ccla.org/wp-content/uploads/2021/06/2018-01-17-Written-submissions-to-SECU-re-C-59.pdf>; and International Civil Liberties Monitoring Group, "Brief on Bill C-59, the *National Security Act, 2017*" (May 2019) at 38, online (pdf): *International Civil Liberties Monitoring Group* <https://iclmg.ca/wp-content/uploads/2019/05/C-59-brief-May-2019-update.pdf>.

<sup>&</sup>lt;sup>34</sup> See e.g., Kate Robertson, Cynthia Khoo & Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (2020), at 15-28, online: *Citizen Lab and International Human Rights Program* <a href="https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf">https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf</a>.

<sup>&</sup>lt;sup>35</sup> See e.g., International Civil Liberties Monitoring Group, Islamic Social Services Association, and Noor Cultural Centre, "Islamophobia in Canada: Submission to the UN Special Rapporteur on Freedom of Religion or Belief" (November 2020), online: OHCHR <https://www.ohchr.org/Documents/Issues/Religion/Islamophobia-AntiMuslim/Civil%20Society%20or%20Individuals/Noor-ICLMG-ISSA.pdf>; Reem Bahdi, "No Exit: Racial Profiling and Canada 's War against Terrorism" (2003) 41:2-3 Osgoode Hall Law Jounrnal 293; Ashley Burke & Kristen Everson, "A Muslim former intelligence officer says systemic racism at CSIS is a threat to national security Social Sharing", CBC (29 June 2021), online: <https://www.cbc.ca/news/politics/racism-descrimination-claims-canadian-security-intelligenceservice-1.6083353>; Tabasum Akseer, "Understanding the Impact of Surveillance and Security Measures on Muslim Men in Canada" (2018), at 45-85, online (pdf): Centre for International and Defence Policy (Queen's University)



- 39. The situation is such that victims/survivors of abuse, especially if they or the perpetrator are Black, Indigenous, or otherwise racialized or are vulnerable across multiple categories of oppression, will often avoid seeking aid from government institutions or calling the police because they do not want to be, or do not want the perpetrator to be, criminalized or subjected to police violence.<sup>36</sup> Tying automated police and national security agency intervention to their online spaces may only serve to isolate victims/survivors further, reducing their ability to seek help from their respective communities or through informal channels.
- 40. With respect to women (cis- and trans-), non-binary individuals, and other gender-diverse people, the disgraceful track record of law enforcement responses to both TFGBV and non-technology-facilitated sexual harassment and assault provides ample evidence to support fears of automated police and intelligence agency involvement in content moderation.<sup>37</sup> This is even more so considering that much online abuse and actual or perceived hate speech targeting women, gender-diverse people, and LGBTIQ+ individuals is sexualized, involves sexual harassment, or attempts to weaponize the targeted individual's sexuality against them.<sup>38</sup> Adding on a layer of technological and sociotechnical illiteracy among law enforcement,<sup>39</sup> in the context of online abuse and vulnerable marginalized individuals, portends nothing short of a recipe for disaster.

# G. New CSIS Powers Are Unjustified and Inappropriately Included in this Consultation

41. For reasons that remain unclear, the government has seen fit to bury new powers for CSIS at the end of a paper ostensibly about platform regulation in relation to certain categories of harmful content,

- <sup>36</sup> See e.g., Amanda Couture-Carron, Arshia U Zaidi & Nawal H Ammar, "Battered Immigrant Women and the Police: A Canadian Perspective" (2021) International Journal of Offender Therapy and Comparative Criminology 1; and Alexa Dodge, "Deleting Digital Harm: A Review of Nova Scotia's CyberScan Unit" (August 2021), at 22-23, online (pdf): VAW Learning Network <a href="https://www.vawlearningnetwork.ca/docs/CyberScan-Report.pdf">https://www.vawlearningnetwork.ca/docs/CyberScan-Report.pdf</a>.
- <sup>37</sup> See e.g., Robyn Doolittle, "Unfounded: Why Police Dismiss 1 in 5 Sexual Assault Claims as Baseless", *Globe and Mail* (3 February 2017), online: <https://www.theglobeandmail.com/news/investigations/unfounded-sexual-assault-canadamain/article33891309>; Robyn Doolittle, "Unfounded: What It's Like to Report a Sexual Assault", *Globe and Mail* (17 March 2017), online: <https://www.theglobeandmail.com/news/investigations/what-its-like-to-report-a-sexualassault-36-people-share-their-stories/article34338353>; and Cynthia Khoo, "Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence" (2021), at 207, online (pdf): *Women's Legal Education and Action Fund (LEAF)* <https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf>.
- <sup>38</sup> See e.g., Cynthia Khoo, "Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence" (2021), at 16, online (pdf): Women's Legal Education and Action Fund (LEAF) <a href="https://www.leaf.ca/wpcontent/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf">https://www.leaf.ca/wpcontent/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf</a>>.
- <sup>39</sup> See e.g., Cynthia Khoo, Kate Robertson & Ronald Deibert,, "Installing Fear: A Canadian Legal and Police Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications" (June 2019), at 165-67, online (pdf): Citizen Lab <a href="https://citizenlab.ca/docs/stalkerware-legal.pdf">https://citizenlab.ca/docs/stalkerware-legal.pdf</a>>.

Болан на споста в Поблатила Босатисти себяната воссоточето ИВ Иссерен астанататели

<sup>&</sup>lt;https://www.queensu.ca/cidp/sites/webpublish.queensu.ca.cidpwww/files/files/publications/Martellos/Martello42E N.pdf>; and Petra Molnar & Lex Gill, "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System" (2018), at 19, online (pdf): *International Human Rights Program and the Citizen Lab* <a href="https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf">https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf</a>>.



despite a tenuous relationship between these powers and the purported objectives of the consultation. There are several problems related to this portion of the proposal, which we discuss below.

- 42. First, in addition to the previously presented concern of violative and discriminatory intrusions into people's lives resulting from mandatory reporting, a related concern is the inability of impacted individuals to seek legal recourse where they are inappropriately targeted by CSIS through OCSPs. In the case of CSIS's security intelligence investigations (section 12 of the CSIS Act) or foreign intelligence investigations (section 16 of the CSIS Act), individuals who have their information disclosed to CSIS may never be able to contest such disclosures, or contest how that information is ultimately used by CSIS. This is in contrast to the context where law enforcement has brought criminal charges against an individual, and there is a greater possibility (comparatively speaking) of contesting the use of information which was disclosed to law enforcement based on information from an OCSP. Thus, the mandatory information sharing scheme proposed combines what will be almost certain inappropriate targeting of individuals by CSIS, with a negligible ability (as compared to in the law enforcement context) to seek legal recourse when unfairly impacted by such investigations. This concern might be mitigated if the government were to require OCSPs to transmit material exclusively to designated law enforcement agencies, instead of CSIS; however, we emphasize that there should be no mandatory reporting as described in the consultation materials in the first place, and that this was an entirely Inappropriate context in which to seek expanded powers for CSIS.
- 43. Second, Canadian academics have robustly demonstrated that Canada suffers from a severe "intelligence to evidence" problem that is often linked to CSIS being unable or unwilling to communicate information to law enforcement bodies due to concerns that doing so will compromise sources or methods.<sup>40</sup> This results in either defendants in criminal cases being robbed of their due process rights, or the inhibition of criminal prosecutions where there is otherwise reason for them to proceed. Again, this issue might be addressed by limiting OCSP information-sharing to law enforcement agencies, but we stress that any legislation purporting to set up new information-sharing channels among or between law enforcement, intelligence agencies, and digital platforms or other technology companies *must* be the subject of its own dedicated public consultation process.
- 44. Third, we oppose the proposal to grant CSIS a new warranting power on the basis of the consultation materials provided. If the CSIS Act were modified, as proposed, the Service would broaden its foreign intelligence operations collection capacity by being able to collect basic subscriber information without having to satisfy section 21 warranting requirements, compared to if section 21 were reformed

<sup>&</sup>lt;sup>40</sup> For some of this discussion, see: Kent Roach, "The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation between Intelligence and Evidence" in *Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182* (2010), available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1629227>; Kent Roach, "The eroding distinction between intelligence and evidence in terrorism investigations" in *Counter-Terrorism and Beyond*, eds Nicola McGarrity, Andrew Lynch & George Williams (Abington: Routlege, 2010); Leah West, "The Problem of 'Relevance': Intelligence to Evidence Lessons from UK Terrorism Prosecutions" (2018) 41:4 Manitoba Law Journal 57; Craig Forcese & Leah West, "Threading the Needle: Structural Reform & Canada's Intelligence-to-Evidence Dilemma" (2019) 42:4 Manitoba Law Journal 131; and Dave Murray & Derek Huzulak, "Improving Intelligence to Evidence (I2E) Model in Canada" (2021) 44:1 Manitoba Law Journal 181.

TORONTO

to include a data production power. This is extremely problematic, firstly, on the grounds that the online harms consultation should not seek to reform how foreign intelligence operations are undertaken and, secondly, on grounds that the government has not demonstrated a clear reason for why data production powers cannot be added to existing section 21 restrictions, as opposed to being provided with a reduction in the court's oversight concerning such new proposed powers. We also note that expanded powers were already granted to CSIS not even five years ago, in the passage of Bill C-59.<sup>41</sup>

- 45. It is not evident from the "Technical Paper" why basic subscriber data production powers could not be added to the existing section 21 regime, as opposed to under a separate unique regime. While the government indicates an issue with timeliness in conducting investigations and a desire for flexibility in operations, it has not demonstrated that section 21 is actually impeding investigations. Again, should this be the case, then the government should hold formal public consultations on national security as opposed to integrating these debates within a broader consultation that primarily concerns completely separate areas of law, scholarship, and expertise. The totality of online expression collectively captured by the consultation materials' proposed five categories far exceeds the national security context or the scope of CSIS's mandate.
- 46. There may be a debate worth having about CSIS's ability to obtain basic subscriber information pertaining to foreign actors that are allegedly engaged in terrorism-related activities associated with inciting terrorist attacks. However, this consultation—which is, at its heart, focused on the role and responsibilities of digital platforms in the context of intermediary liability law, content moderation, online abuse, and technology-facilitated gender-based violence, abuse, and harassment—does not provide the appropriate forum to do so.
- 47. Fourth, we oppose the proposed *CSIS Act* modification on grounds that the proposed reforms would weaken Federal Court oversight of CSIS operations at a time where the Service has exhibited a chronic failure to meet its existent obligations to behave with candour towards the courts.<sup>42</sup> There is ample public evidence demonstrating that CSIS and its counsel have actively misled the Federal Court in relation to CSIS's activities and operations. This misconduct should not be rewarded with weakened judicial oversight to obtain new classes of information by way of evading the requirements present under the existing section 21 regime. At the very least, any data production powers that are meant to facilitate section 16 activities should fall under section 21 of the *CSIS Act* instead of operating under a separate regime—but again, no national security legislative reform should occur as a result of this consultation.

Колан на селота в Поблатила Составал селота воссовать с НЕ Черета селотаталова — с

Catharine Tunney, "Canada's national security landscape will get a major overhaul this summer", CBC (23 June 2019), online: <a href="https://www.cbc.ca/news/politics/bill-c59-national-security-passed-1.5182948">https://www.cbc.ca/news/politics/bill-c59-national-security-passed-1.5182948</a>>.

<sup>&</sup>lt;sup>42</sup> See e.g., Jim Bronskill, "Court admonishes CSIS once again over duty of candour", *Globe and Mail* (31 August 2021), online: <a href="https://www.theglobeandmail.com/canada/article-court-admonishes-csis-once-again-over-duty-of-candour">https://www.theglobeandmail.com/canada/article-court-admonishes-csis-once-again-over-duty-ofcandour</a>>.



#### Басцинал селиментир на слава Гация цата автода в Триболистир Босолисти переора босно ила со Вла чесева на млаготите на

OF GLOBAL AFFAIRS & PUBLIC POLICY

# H. Conclusion: Rewrite the Proposal from the Ground Up

- 48. For all of the reasons detailed above, we strongly recommend that the federal government revise, in earnest, this particular piece of proposed legislation, from the ground up. It is not too late to change course, and to incorporate recommendations that reflect what civil society groups and technology and human rights experts have been communicating directly to the responsible ministries and departments over the course of the past several years—alongside representatives of the purported beneficiaries of the proposed legislation, such as historically marginalized groups targeted by TFGBV.
- 49. At the very least, the proposed measures should be broken up into two or more separate pieces of legislation—if not a separate legal regime tailored to each of the five designated categories, then perhaps one specific to NCDII and/or child sexual exploitation materials, and a separate scheme (or schemes) addressing hate speech, terrorist content, and/or incitement to violence. That separation would result in more internally coherent proposals, fewer constitutional complications, and more honest and precise debates regarding each of the five content categories on their own merits, rather than being dangerously and counterproductively conflated with each other. The government would be more likely to achieve its purported objectives in that case, whereas the currently proposed measures will only set up all involved for failure, at the expense of those already being harmed the most.

hanstanten erstendet half son Sonalen her de groei de Seis Unikog de hans hanstagen gebreiken son keregen andere Die die erste de oanstanten de so



#### Response to the Government of Canada's Proposed Framework for Regulating Harmful Content Online September 2021

# **Executive Summary**

Microsoft welcomes the opportunity to provide its comments in response the Government of Canada's proposal for regulating harmful online content set out in the government's <u>Discussion Guide</u> and <u>Technical</u> <u>Paper</u> (the "Online Harms Proposal" or "Proposal"). We recognize that government regulation has an important role to play in addressing digital safety, and we support the development of a principled and carefully calibrated regulatory framework. We also commend the Government of Canada for making a commitment to "confronting online harms while respecting freedom of expression, privacy protections, and the open exchange of ideas and debate online". Any regulation meant to promote digital safety must also protect human rights and preserve the free and open internet.

There is an opportunity for the Government of Canada to develop world-leading digital safety legislation through the development of targeted, proportionate measures to address illegal content online while protecting human rights. To help achieve this balance, we suggest recalibrating some elements of the Online Harms Proposal, including the following:

- <u>The scope of services to be covered</u>: The Online Harms Proposal (at least initially) should focus only on the services that pose the greatest risk (certain social media networks and video-sharing platforms). Additional service types could potentially be added over time, in accordance with clearly defined criteria.
- <u>The scope of content to be covered</u>: The regulation of particular content, including the issuance of mandatory removal orders, should be limited to content that is illegal in Canada. Legal but potentially harmful content should remain subject to the content moderation procedures adopted by service providers, in accordance with their own terms of service and other policies.
- <u>The obligations on service providers</u>: Service providers should not be required to proactively monitor user content, nor decide whether particular content is unlawful. Elected officials and independent courts – not private companies – should be the decision-makers on which content is illegal.
- <u>The availability of safe harbour protections</u>: Service providers should have intermediary liability immunity to allow them to carry out good-faith content moderation and other actions to enhance digital safety. Safe harbour protections should apply equally to actions taken to comply with law, as well as "good Samaritan" voluntary measures.
- <u>The powers delegated to the Digital Safety Commissioner</u>: Powers delegated to the Digital Safety Commissioner (the "Commissioner") should be scaled back to better recognize the potential human rights' impacts of decisions taken under digital safety legislation, to place limits on inspection and order-making powers, and to provide greater transparency and oversight by Parliament.

Recalibrating the Online Harms Proposal in these ways will not undermine the Government of Canada's efforts to enhance digital safety. To the contrary, these changes can help the government achieve its vision of confronting online harms while respecting freedom of expression, privacy protections, and the open exchange of ideas. Equally, adopting these recommendations can help ensure Canada's digital safety regulation is pragmatic, proportionate, and effective.

# Introduction

# The importance of digital safety at Microsoft

Microsoft recognizes that technology companies have a special role to play in helping make the internet safer for individuals. We also acknowledge that service providers should seek to design and operate their services in responsible ways, while anticipating and reducing digital safety risks unique to their services.

Microsoft has a long-standing commitment to digital safety, as well as a history of working closely with governments, industry, civil society organizations, and academics to reduce the presence of illegal and harmful online content. Microsoft's <u>PhotoDNA</u> tool is used by many leading technology companies and law enforcement to scan for and remove, child sexual exploitation and abuse imagery from online platforms and services. Microsoft has supported the Voluntary Principles to Combat Online Child Sexual Exploitation and Abuse and is a member of both the Technology Coalition and the WeProtect Global Alliance. Microsoft is also a founding member of the Global Internet Forum to Counter Terrorism and has committed to the "Christchurch Call To Action To Eliminate Terrorist and Violent Extremist Content Online". In 2018, Microsoft launched the Defending Democracy Program, an innovative effort to protect our democratic institutions and processes from hacking, increase political advertising transparency online, explore technological solutions to preserve and protect electoral processes, and defend against disinformation campaigns. Microsoft is also a member of the Digital Trust and Safety Partnership, an industry initiative committed to developing best practices to ensure consumer trust and safety when using digital services.

# The role and nature of government regulation

Digital safety is a whole-of-society problem that needs a whole-of-society solution. All stakeholder groups need to do more to address the issues of illegal and harmful content online. While we are proud of our digital safety work, we recognize that voluntary industry efforts are not always sufficient to address the full range of harms online. Government regulation has an important role to play, and we support the development of principled and carefully calibrated regulatory efforts to enhance digital safety.

Regulatory frameworks should balance the legitimate interests of individuals, businesses, and society as a whole. While it is critical to enhance digital safety, a delicate balance must be struck to ensure that government regulation does not undermine freedom of expression, privacy protections, and the open exchange of ideas. Efforts to enhance digital safety should also be effective and proportionate, while not undermining other important public policy objectives, including growth of the digital economy, the scaling up of start-up businesses, and access by consumers to digital products or services.

To be effective and proportionate, digital safety regulations need to take into account what service providers and other stakeholders can feasibly implement and maintain from an operational and technical perspective, as well as how regulatory compliance can be achieved through globally applied solutions that are tailored to national laws.

September 2021

# Principles-based approach to online safety regulation

As a global company, Microsoft has developed a set of harmonized safety principles that inform our thinking on regulatory developments across jurisdictions. We encourage the Government of Canada to consider these principles as it considers how to achieve its vision for a safe, inclusive and open online environment.

- 1. <u>Operate responsibly</u>. Providers of digital services play an essential role in promoting digital safety. That means they have an obligation to design and operate their services in responsible ways that anticipate and reduce digital safety risks unique to their services.
- 2. <u>Respect the fundamental rights of all people</u>. The internet is a key enabler of human rights, among them the fundamental right of freedom of expression. It also allows users to access information from a range of sources. Any regulation meant to promote digital safety must also protect these important human rights by preserving the free and open internet.
- 3. <u>Maintain an open internet</u>. Obligations to address digital safety risks should not force digital services to become content gatekeepers. The ability of users to create and share content directly and immediately is what makes the internet so dynamic and enables access to the broadest possible range of information. Although digital services have a responsibility to operate their services safely, making them responsible for what their users say, post, search for, or link to would, for practical purposes, undermine how many services on the internet work and destroy the internet's essence and value.
- 4. <u>Draw the line between illegal and harmful content</u>. Regulation of particular content, including mandatory blocking orders, should be limited to that which government defines as illegal. Elected officials and independent courts—not private companies—should be the decision-makers. They should also be the guarantors of due process where a balancing of rights is required, applying internationally agreed norms and longstanding human rights principles. Regulation to address other digital safety risks associated with harmful, but not illegal, content should focus on systems and processes, including digital services' compliance with their own digital safety commitments to users.
- 5. <u>Embrace clarity and transparency</u>. Any government regulation of content online should clearly define what is regulated and on what services. Ambiguity will chill speech and also force digital services to make subjective decisions on what content to block, what conduct to punish, and under what circumstances. Just as any government regulation should reduce ambiguity, digital services should provide clarity and transparency about their digital safety commitments to users, decision-making processes and enforcement actions.
- 6. <u>Harmonize laws wherever possible</u>. Regulation of online content should be harmonized across jurisdictions wherever possible. The global internet benefits everyone. Because of the borderless nature of many digital services, regulatory fragmentation will splinter the internet, deprive users of access to information, and leave digital services less able to protect their users from harm. Regulations that force the creation of country-specific infrastructure to be built and maintained both make it more likely for geo-filtering to be used by foreign service providers to prevent access to their services from within specific jurisdictions and undermine efforts of domestically-delivered

services to compete globally. These risks may be disproportionately impactful for Canada - both because of its small population and ambition to become a leading jurisdiction for digital and online businesses selling into the global marketplace.

- 7. <u>Recognize that there's no silver bullet...</u> Digital services should adopt and follow safety-enhancing systems and processes that will be most effective for their services. The law should not, however, require adoption of a specific technology solution nor assume technology exists to solve every problem. There is no technology solution that will keep users absolutely safe.
- 8. <u>... and there's no one-size-fits-all solution</u>. Providers' obligations should be tailored to the nature of their services, taking into account the function of the service, relationship between provider and end users, expectations of users, and risk profile of the service itself. In other words, productivity tools should not be treated the same as general purpose social media services.
- 9. <u>Incentivize positive action</u>. Regulation should incentivize digital services to take voluntary steps to protect users from exposure to illegal or harmful content. Furthermore, where digital services act reasonably and in good faith to do more than the law requires, they should not be assumed to acquire "knowledge" of content that then subjects them to liability.
- <u>Engage the whole of society</u>. The fact that criminals and other bad actors weaponize the internet isn't a "technology" problem, or one that the tech sector alone should address. Digital safety requires a whole-of-society approach based on shared responsibilities among services, users, and public authorities.

# Specific recommendations on the Online Harms Proposal

While we support the government taking an active role to enhance digital safety, we have concerns that the current Online Harms Proposal could have disproportionate impacts on freedom of expression and other fundamental human rights. Related impacts of the Online Harms Proposal will be felt both inside Canada and internationally, particularly if countries without strong democratic institutions point to Canada's approach in defense of regulatory frameworks within their borders that are used to crack down on internet speech or other human rights. We recommend that policymakers consider the potential precedent setting impact of this legislation and how it aligns with Canada's wider policy positions on a free, open and secure internet.

We are also concerned that the Online Harms Proposal may not be effective. The current Proposal risks going too far in regulating online services and content, which may have disproportionate and unintended consequences for Canadian citizens and businesses.

To effectively address online harms while protecting human rights and Canada's economic and other policy interests, we recommend recalibrating the Online Harms Proposal in at least the five respects set out below.

#### Recommendation 1:

The Online Harms Proposal (at least initially) should focus only on the services that pose the greatest risk (general purpose social media networks and video-sharing platforms). Additional service types could potentially be added over time, in accordance with clearly defined criteria.

Microsoft

The Technical Paper defines regulated "Online Communication Services" by reference to whether the "primary" purpose of the service is to enable users to communicate with other users of the service over the internet. The paper specifically excludes: (a) services that enable persons to engage only in private communications; (b) businesses that provide only a telecommunications service; and (c) search engines.<sup>1</sup> The Discussion Guide also indicates, by way of example, that online communications services will not include fitness applications or travel review websites, presumably on the bases that user communications within those services are not the primary purpose of the service.

Even with these exclusions, the definition of Online Communications Services casts a wide net, as it would capture a broad range of online services, including services with a small number of users, that involve communications of little (if any) illegal or harmful content. For example, the definition could arguably capture communication services created to allow regulated professionals, such as doctors or lawyers, to share information or insights. By broadly defining Online Communication Services and not focusing on services with higher risk profiles or features, the Online Harms Proposal adopts a disproportionate approach that is not tailored to reducing the online harms that it is intended to address. This approach increases the likelihood that a broad range of service providers will implement conservative content moderation measures that may remove lawful and contextually relevant content. It also creates significant roadblocks for emerging service providers (who will often lack the financial and operational resources needed to effectively ensure compliance while also balancing the risks to freedom of expression, privacy and human rights), thereby entrenching the position of established players.

To address these concerns, we recommend revising the definition of Online Communication Services to make clear that the obligations in the legislation will apply, at least initially, to the services most likely to be used to share or spread illegal or harmful content: general purpose social media and video-sharing services with the following characteristics:

- Facilitate socialization or social networking of all types;
- Offer the option for users to interact with or discover unknown people, or groups with shared interests;
- Leverage recommender systems (i.e., fully or partially automated systems used to suggest content or information to users of the service) to promote certain content, with the business objective that the content could be spread virally; and
- Have achieved high participation rate (i.e., monthly active users over a specified amount; e.g., 10% of the Canadian population).

Modifying the definition in this way will help ensure that Canada's regulatory framework is aligned with the principles of necessity and proportionality, while helping to reduce unintended consequences. These consequences may include, for example, reduced access to products or services by consumers in Canada – due to geo-filtering by service providers who lack the financial resources or business case to create new digital interfaces and procedures for a small market, and reduced competitiveness of Canada's technology sector – due to the need to build and maintain digital tools and operational procedures that are unique to

<sup>&</sup>lt;sup>1</sup> Defined in Section 4 of the Technical Paper as: "a person who indicates the existence or location of content or hosts or caches the content or information about the location of the content, by reason only that another person uses their services to provide an Online Communication Service".

Canada. We believe that regulation should preserve the space for competition in the market by ensuring it does not create such high barriers to entry that none but the largest providers can compete.

Recalibrating the scope of services subject to regulation in this way would not diminish the effectiveness of Canada's regulatory framework. Rather, it would ensure that regulatory obligations are directed at the online communications services that are the focus of the Discussion Paper – namely, general purpose social media and video-sharing networks. It will also enable the Government of Canada to more effectively tailor the regulation to the services that are in scope, which reduces the risk of measures applying to low-risk services with fundamentally different purposes, features, or audiences.

Additionally, it would not prevent the government from regulating other categories of online communication services in the future if required to advance the goals of the legislation and to keep up with changing technology. To provide the government with flexibility going forward, the Governor in Council could have (as described in Section 3 of the Technical Paper) the authority to "make regulations [...] specifying a category of services that is to be included within the regulatory framework, notwithstanding that it does not meet the definition of OCS, if the Governor in Council is satisfied that there is a significant risk that unlawful or harmful content is being communicated on the category of services or that specifying the category of services of the Act". It may also be appropriate to add other criteria so as to provide certainty to providers – especially those developing new services.

# Recommendation 2:

The regulation of particular content, including the issuance of mandatory removal orders, should be limited to content that is illegal in Canada. Legal but potentially harmful content should remain subject to the content moderation procedures adopted by service providers, in accordance with their own terms of service and other policies.

The Online Harms Proposal adopts an expansive approach to the scope of content to be regulated. It contemplates legislation that includes definitions for the following five categories of harmful content:

- Terrorist content;
- Content that incites violence;
- Hate speech;
- Non-consensual sharing of intimate images; and
- Child exploitation content.

The Proposal indicates that these categories of content are to be defined in a way that borrows from the *Criminal Code*, but are adapted to the regulatory context. It is not evident what this will mean in the future legislation, but the Proposal does make clear that these definitions may include content that is not criminalized under Canadian law but may still be harmful to at least one Canadian. The Proposal both extends the reach of Canadian law and reduces clarity about what is in scope. In general, we recommend that policymakers draw bright lines between content that is unlawful, versus content that is lawful but potentially harmful – the current proposal would blur these lines.

The expansive approach being proposed by the Government of Canada contrasts with the more measured approach found in the European Union's proposed *Digital Services Act* (the "DSA"). The DSA requires regulated service providers to give effect to orders from national judicial or administrative authorities to

remove illegal content.<sup>2</sup> Additionally, regulated service providers are required to put in place a mechanism allowing users to report content that is illegal, which a service provider may decide to take down – either on the grounds that the content is illegal or that it is contrary to the provider's terms of service.<sup>3</sup>

By restricting the Online Harms Proposal to illegal content (as defined under Canadian law), users and service providers would have greater clarity about what is in scope. It would also help ensure that limitations on online speech and other fundamental rights are necessary, proportionate, and enforceable (see also Recommendation 3 below).

To the extent that the Online Harms Proposal seeks to deal with content that is lawful but potentially harmful, we recommend that it take a systematic and process-based approach, rather than regulating for specific outcomes for specific content. This means encouraging providers to have procedural and substantive mechanisms for due process in content moderation and enforcement and to provide meaningful and actionable transparency. For instance, Microsoft requires users to adhere to our terms of service and code of conduct, which prohibit certain types of content and conduct. Where these are violated, we take enforcement action.

Should lawful but potentially harmful content remain in scope, we strongly recommend considering measures that instead focus on holding service providers accountable for upholding their own policies and commitments to their users. Creating space for appropriate self-regulatory measures may be one approach.

#### Recommendation 3:

Service providers should not be required to proactively monitor user content, nor decide whether particular content is unlawful. Elected officials and independent courts – not private companies – should be the decision-makers on which content is illegal.

The Online Harms Proposal requires regulated service providers to "take all reasonable measures, which can include the use of automated systems, to identify harmful content that is communicated on its service and to make that content inaccessible to persons in Canada."<sup>4</sup> In addition, regulated service providers would be required to independently adjudicate complaints and remove illegal or harmful content within 24 hours from the content being flagged,<sup>5</sup> A failure to comply with these requirements would trigger significant administrative monetary damages.

Both of these obligations impinge on fundamental freedoms enshrined in the *Canadian Charter of Rights and Freedoms* and international human rights law, to the extent that this approach may risk being perceived as a government censorship regime that is outsourced to private companies. Requiring service providers to proactively monitor all user content and to assess the legality or harmfulness of user content is problematic. First, this requirement may have a disproportionate effect on user privacy, and may undermine necessary cybersecurity efforts by effectively eliminating the ability to leverage encryption for certain communications. The extraordinary policy implications merit greater public debate. Second, proactive scanning is not a silver bullet. There are no failsafe technical scanning solutions, particularly as machines are not able to understand

<sup>&</sup>lt;sup>2</sup> DSA, Article 8.

<sup>&</sup>lt;sup>3</sup> DSA, Article 14.

<sup>&</sup>lt;sup>4</sup> Technical Paper, Section 10.

<sup>&</sup>lt;sup>5</sup> Technical Paper, Section 11.

context. Moreover, different types of content may require the use of different scanning technologies. Usage of scanning technologies today risks overcensorship unless there is substantial human oversight and review of flagged content, conducted by large armies of human content moderators. Given the volume of content that is generated on a daily basis, implementing useful proactive scanning technologies is largely impractical and may serve to undermine the dynamism of the internet and the benefits of interconnected online spaces. Third, removing the proactive monitoring obligation would not mean that illegal or harmful content would go unaddressed. Digital safety regulation should take a process-based approach that focuses on ensuring that service providers implement procedures that allow their users to report illegal content in a manner that is effective, accessible and easy to use. By way of example, Canada's digital safety legislation could include a requirement similar to the EU where regulated service providers must put in place a mechanism allowing users to report content that is illegal.<sup>6</sup>

Requiring service providers to adjudicate the legality or harmfulness of content also fails to take into account that service providers are not equipped to make content decisions that require applying legal standards or assessing intent, context and cultural subjectivities. Making judgments on online speech is often a complex process, requiring subject matter expertise and a careful balancing of rights. It is not appropriate for service providers to make these decisions – and the challenges are exacerbated where legislation requires removal within a short, fixed time period. Legally mandated adjudication and takedown rules incentivize service providers to adopt a conservative approach to content removal, which could lead to the disproportionate removal of legitimate content. This, in turn, could have unintended, negative consequences for freedom of expression and risks creating a chilling effect on online speech, free and open public discourse, and civil society participation.

The challenges of making complex and contextual content decisions are further exacerbated if the Proposal retains the obligation for service providers to notify law enforcement if the service provider "has reasonable grounds to suspect that content falling within the five (5) categories of regulated harmful content reflects an imminent risk of serious harm to any person or to property".<sup>7</sup> Although this obligation includes some helpful qualifiers, such as "imminent risk of serious harm", it may be difficult for service providers determine what constitutes a "serious harm", particularly if the government chooses to regulate harmful, and not just illegal, content. We recommend clarifying this obligation so that it only applies to harmful content involving a manifestly clear threat to life or serious bodily harm, and where the provider becomes aware of specific, actionable information, such as time and location of a threatened act.

For these reasons, elected officials and independent courts, not private companies, should be the decisionmakers on the legality of content. Independent courts are the guarantors of due process where a balancing of rights is required and where internationally agreed norms and human rights principles are applied. Significantly, both of these points have informed the approach to content moderation in the EU. The draft DSA expressly states that it should not be construed as imposing "a general monitoring obligation or active fact-finding obligation, or [...] a general obligation for providers to take proactive measures to relation to illegal content."<sup>8</sup> In addition, the obligations on service providers in the DSA to remove content are limited

<sup>&</sup>lt;sup>6</sup> DSA, Article 14.

<sup>&</sup>lt;sup>7</sup> Technical Paper, Section 20.

<sup>&</sup>lt;sup>8</sup> DSA, Article 28.

to complying with takedown orders made by judicial or administrative authorities, not private companies.<sup>9</sup> Microsoft recommends following this practical and balanced approach.

# Recommendation 4:

Service providers should have intermediary liability immunity to allow them to carry out good-faith content moderation and other actions to enhance digital safety. Safe harbour protections should apply equally to actions taken to comply with law, as well as "good Samaritan" voluntary measures.

To advance the government's policy objectives, it is critical that regulated service providers and other intermediaries (i.e., including intermediaries who are not subject to the regulatory framework) do not face liability or any other adverse legal consequences for their good faith efforts to combat and overcome online harms. Safe harbour and immunity provisions should apply to actions taken to comply with regulatory obligations, as well as self-initiated "good Samaritan" voluntary measures that go beyond providers' obligations in the legislative framework.

To be effective, immunity needs to cover the following activities:

- Content moderation and other actions required to comply with law or undertaken voluntarily, such as: (a) monitoring content (where appropriate); (b) assessing compliance with a provider's terms of service; (c) taking reasonable measures to make violating content inaccessible or other enforcement measures, and (d) providing impacted individuals or groups with the opportunity to request that content moderation decisions be reconsidered;
- Notifying law enforcement of content or providing related data that may constitute a crime under Canadian law; and
- Preserving content and related data.

The Technical Paper addresses only one of these activities and provides immunity only to regulated service providers. Specifically, the paper provides that "The Act should provide that OCSPs making (a) notifications to the RCMP or (b) reports to law enforcement and CSIS in good faith pursuant to the Act should have immunity from civil and criminal proceedings."<sup>10</sup>

The limited immunity proposed in the Technical Paper is inadequate, as it leaves regulated service providers and other intermediaries potentially exposed to both civil and criminal proceedings as a result of good faith efforts to comply with their legal obligations or to voluntarily enhance digital safety beyond the strict requirements of the applicable legislation. This limited immunity is problematic generally, but is most concerning to the extent that a legislative framework is enacted that regulates more than just illegal content and requires services providers to make a contextual and legal assessment as to whether specific content needs to be made inaccessible or reported to law enforcement.

By way of comparison, the safe harbour provisions in the EU's DSA are broader. While Canada's safe harbour provision is limited to notifying and reporting to law enforcement, the DSA provides for liability exemptions for intermediaries (including caching and hosting services) when prescribed conditions are met (e.g., in the case of hosting services, lack of knowledge of illegal activity and, upon obtaining such knowledge, acting

<sup>9</sup> DSA, Articles 8.

<sup>&</sup>lt;sup>10</sup> Technical Paper, Section 26.

expeditiously to remove or to disable access to the illegal).<sup>11</sup> The DSA also makes clear that these exemptions apply even in circumstances where an intermediary undertakes voluntary activities or measures to tackle illegal content.<sup>12</sup> In doing so, the DSA provides important incentives for service providers to engage in responsible, good faith efforts to address content moderation and online harms. Similar incentives should be included in any Canadian legislation.

# Recommendation 5:

Powers delegated to the Commissioner should be scaled back to better recognize the potential human rights' impacts of decisions taken under digital safety legislation, to place limits on inspection and order-making powers and to provide greater transparency and oversight by Parliament.

The Technical Paper proposes the creation of a Digital Safety Commissioner with exceptionally broad authority to make orders requiring a regulated service provider to do any act or thing, or refrain from doing any act or thing necessary to ensure compliance with the service provider's regulatory obligations.<sup>13</sup> The Commissioner would also have responsibility for recommending that administrative monetary penalties be imposed by the Personal Information and Data Protection Tribunal.<sup>14</sup> These powers are enabled through the authority to conduct inspections of regulated service providers at any time, on either a routine or ad hoc basis, at the Commissioner's own discretion (and even if there is no reasonable basis to believe that the service provider is in violation of the law).<sup>15</sup> These inspection powers are wide-reaching, allowing an inspector to enter any place in which they believe there is any document, information or any other thing, including computer algorithms and software, relevant to verifying compliance or preventing non-compliance.<sup>16</sup> Any of these things can be removed for examination or reproduction, presumably without regard to other legal obligations or privileges associated with users or with providers.

The Technical Paper also proposes that the Commissioner have broad regulation-making powers, allowing the Commissioner to prescribe:

- What measures must be taken to identify harmful content or make it inaccessible;
- What mechanisms need to be in place to flag harmful content or dispute a flag;
- What content-moderation guidelines need to be published;
- What amount and kind of data and information needs to be preserved;
- What regulated service providers must do to comply with the regulatory framework; and
- What regulatory charges one or more classes of regulated service providers must pay.

Both individually and taken together, the proposed powers of the Digital Safety Commissioner lack reasonableness and proportionality. The Proposal risks vesting excessive power in an unelected official, without appropriate due process protections or other guardrails. They also risk the creation of prescriptive, one-size-fits-all measures. To address these concerns, powers delegated to the Commissioner should be scaled back to better recognize the potential human rights' impacts of decisions taken under digital safety

<sup>&</sup>lt;sup>11</sup> DSA, Article 5.

<sup>&</sup>lt;sup>12</sup> DSA, Article 6.

<sup>&</sup>lt;sup>13</sup> Technical Paper, Section 80.

<sup>&</sup>lt;sup>14</sup> Technical Paper, Section 104.

<sup>&</sup>lt;sup>15</sup> Technical Paper, Section 88.

<sup>&</sup>lt;sup>16</sup> Technical Paper, Section 89.

legislation, to place limits on inspection and order-making powers and to provide greater transparency and oversight by elected officials. In particular, we offer the following recommendations:

- <u>Regulation-making powers</u>. Elected officials (represented through the Governor-in-Council), rather than the Commissioner, should be vested with authority to promulgate regulations under the legislation. Government curtailment of citizens' freedom of expression merits accountability directly to those citizens.
- Impact and feasibility assessments. The Commissioner should be required to complete and publish an assessment of human rights' impacts and feasibility (including technical constraints) in respect of any compliance guidelines, measures or decisions issued by the Commissioner. This assessment should, when appropriate, be based on a consultative, multi-stakeholder process.
- Inspection powers. Limits and clarity should be introduced on the categories of information that . the Commissioner may gather. The circumstances in which inspection powers may be exercised should be restricted to align with the audit powers in the Personal Information Protection and Electronic Documents Act (i.e., situations in which the Commissioner has reasonable grounds to believe that the organization has contravened a material regulatory obligation). The Commissioner's use of the information or documents obtained through an inspection should be limited to completing the investigation. Similarly, the Commissioner should be required to maintain the confidentiality of this information, subject to reasonable exceptions for disclosures that are required in connection with the investigation, and the Commissioner should be expressly required to respect legal privilege. Like under the Personal Information Protection and Electronic Documents Act, the Commissioner should also return any information or documents that were obtained through an inspection within a prescribed time period upon request from the service provider.<sup>17</sup> In no circumstances should a service provider be required to provide information if doing so would cause it to violate another law applicable to its operations, including a law in another jurisdiction. To avoid an apprehension of bias, and similar to a requirement that applies to the Canadian Radiotelevision and Telecommunications Commission, the Commissioner should be required to establish two independent arms - one arm that is vested with inspection and investigative responsibilities and a second arm that is responsible for exercising other powers of the Commissioner.
- Order-making powers. The authority of the Commissioner to issue orders should be limited to the same circumstances where a court would issue an interlocutory injunction (i.e., where irreparable harm may occur if an order is not made and the balance of convenience favours the making of the order). To ensure due process, all other orders should be made by the Personal Information and Data Protection Tribunal. There should be a right of appeal to a court of any order or decision of the Personal Information and Data Protection Tribunal Information and Data Protection Tribunal (similar to appeal rights under the *Competition Act* and the *Broadcasting Act*).
- <u>Transparency</u>. In addition to the Commissioner's annual report contemplated in Section 77 of the Technical Paper, the Commissioner should be required to issue transparency reports to Parliament that might include, for example, details on the number and type of notices that have been issued, formal warnings issued, information sought by the Commissioner from regulated service providers, and the processes followed to exercise the Commissioner's powers. Transparency reports should

<sup>&</sup>lt;sup>17</sup> Section 18(3) of the Personal Information Protection and Electronic Documents Act states: "*The Commissioner or the delegate shall return to a person or an organization any record or thing they produced under this section within ten days after they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced.*"

include an assessment of how fundamental rights and freedoms have been balanced with decisions and enforcement actions of the Commissioner.

## Conclusion

It is clear that legislators and policymakers in Canada and elsewhere face significant challenges when developing legislation designed to enhance digital safety without undermining the fundamental rights and freedoms of individuals, and that support other important policy and societal objectives. There is much at stake – for individuals, for businesses, and for governments. The impacts of digital safety legislation are not limited to a single country, as a legislative framework that fails to protect human rights may embolden countries with poor human rights records to use "safety" legislation to limit freedom of expression, privacy rights and the open exchange of ideas.

We believe strongly that implementing the recommendations in this submission will not undermine the Government of Canada's efforts to enhance digital safety. To the contrary, implementing them will be critical if the government is to achieve its vision of effectively confronting online harms while respecting fundamental rights and freedoms.

Microsoft thanks the Government of Canada for the opportunity to make this submission. We look forward to continuing to engage in the government's consultative process and would welcome the opportunity to share with you our perspective on important policy issues related to the Proposal that are not addressed in our submission, including website blocking orders and algorithmic transparency.



September 20, 2021

### The Federal Government's Proposal to Address Online Harms: Recommendations for Children's Safety Online

By: The Centre for Media, Technology and Democracy

Commented On: The Federal Government's proposed approach to address harmful content online

On July 29, 2021, the Federal Government announced its proposal to set "new rules" obliging "Online Communication Service Providers" (OCSPs) to address five categories of harmful content on their platforms: hate speech; child sexual exploitation content; non-consensual sharing of intimate images; incitement to violence content and terrorist content. The legislation requires OCSPs "take all reasonable measures" (including automated filtering and ISP website blocking as a last resort) to identify and block these five categories within 24 hours of being flagged, while also providing procedural transparency to users and survivors.

While we share significant concerns about the wide scope; 24-hour takedown requirement; proactive monitoring of *all* harmful content; and website blocking with <u>Canadian</u> and <u>international</u> experts alike, we raise additional concerns about the lack of consideration of children's rights in the upcoming online harms legislation. We highlight Canada's duty of care to protect children from harmful content online, to impose age-specific requirements, and to mandate provisions for special categories of harmful content, including altered sponsored and paid content.

A growing number of civil society groups, lawmakers and governments around the world have established that *all* online governance <u>should consider children's rights</u>. This note offers a few key areas of concern pertaining to children's safety and well-being online that Canada should consider in its "approach to addressing harmful content online."

1. Recognize duty of care toward 'best interest of the child' in all online regulation and mandate 'best interest of the child' as the primary consideration when in conflict with commercial interests

While Canada is a signatory of the <u>United Nations Convention on the Rights of the Child</u> (<u>UNCRC</u>) it has yet to formally acknowledge and uphold its duty to afford special protections to children established in such international human rights law frameworks in its upcoming plans to "address harmful content online." Such special protections should include i) the 'best interest of the child' as set out by general comment No.25 of the UNCRC and ii) protecting children from encountering harmful content.

i) Defined in Article 3 of the UNCRC, the 'best interest of the child' should "be a primary consideration in all decisions to regulate online activity" by incorporating provisions that protect children's safety, health, wellbeing, psychological and emotional development, identity, freedom of expression and agency to form individual views, among others. Countless civil society organizations around the world have advocated for the 'best interest of the child' and the United Kingdom recently demonstrated its commitment to take them seriously -- especially when children's interests stand in contrast to commercial interest. The new <u>Age Appropriate Design Code</u> mandates websites and apps take the "best interests" of their child users into account when designing and developing online services likely to be accessed by a child, or face fines of up to 4% of annual global revenue. These services span a wide range of social media platforms, video and music streaming sites, as well as gaming apps and sites.

In April 2021, the <u>Alliance for Protecting Children's Rights and Safety Online</u> addressed specific recommendations to proactively protect children from harm to Prime Minister, Justin Trudeau. The Alliance <u>recommends</u> that the 'best interest of the child' be a primary consideration by incorporating specific provisions for "**all** products and services likely to impact children – not only for those directed at them."

So far, the published federal guides include instructions for children only in provisions around child sexual exploitation, in alignment with Canada's Criminal Code. While of utmost importance, the proposal leaves a wide array of other online harms to children's safety, well-being, health and psychological and emotional development unattended.<sup>1</sup> These harms include content and communication which promotes medical misinformation, incitements to violence and radicalization, and harmful activities such as suicide, self-harm and disordered eating, to name only a few.

As such, specific categories for the scope and definition of online harms as they pertain to children should be built into Canada's upcoming proposal, including age-specific obligations.

The Centre for Media, Technology and Democracy

<sup>&</sup>lt;sup>1</sup> This note is primarily concerned with harmful content which is outside the scope of child sexual exploitation as defined by Canada's Criminal Code.

#### 2. Break down online harms proposal into specific legislation for children's rights and protection from harmful content online

Mandating specific requirements and duties of care for age-appropriate <u>design</u> <u>standards</u> for children online would support broader recommendations to break down Canada's proposal into subject-matter specific legislation as legal experts <u>Cynthia Khoo</u> and <u>Emily Laidlaw</u> advocate. Narrowing the scope of online harms would also address a key point of public contention about the overly broad sweep of Canada's current proposal. Carving out special categories of harm to children beyond criminal offences would also align Canada's upcoming proposal with leading global regulation in this space.

For instance, the recent <u>United Kingdom's Online Safety Bill</u> includes "services likely to be accessed by children" as one of three separate categories of harm. The duties for this children-specific category include taking proportionate measures to mitigate and manage the risk and impact of harms to children in different age groups as well as preventing children of *any* age from encountering certain material alongside preventing specific age groups who might be at risk of harm from encountering harmful content.

The UK Online Safety Bill includes requirements for companies to carry out risk assessments and adhere to "safety duties" for each category of harm. By carving out more specific categories of harm, Canada could impose child safety and wellbeing risk assessments which would account for both harmful content as well as the systems which promote and amplify the spread of harmful content, including algorithms and other functionalities for circulating content. While not without limitation, risk assessments are crucial accountability mechanisms for preventing harm *before* they occur.

 Canada's upcoming legislation should include strict requirements to i) minimize children encountering manipulated images of facial and body features in paid and sponsored content and should ii) mandate strict disclosure of manipulations to facial and body features in paid and sponsored content.

Given the growing number of self-harms, harms to mental health and body image, and disordered eating resulting from the consumption of visually modified content online, Canada should account for images with manipulated facial and body features as specific categories of risk and mandate reasonable provisions to minimize their harm, including clear disclosure and content labels. This reflects a growing global commitment

з

to address the promotion of unrealistic body image standards to children and young people.

In Norway, for instance, anorexia is the third most common <u>cause of death</u> among young girls. The country has recently enforced legal disclosure for advertisements that have been photoshopped or otherwise manipulated, including "<u>enlarged lips, narrowed</u> <u>waists, and exaggerated muscles</u>." In Canada, where <u>suicide rates</u> are the leading cause of death for children aged 10 - 14, preventing undue risk from encountering unrealistic body images should be of top priority for the federal government. The government should at minimum extend further consultations with children's health and safety experts and advocacy groups before enacting harmful content legislation.

# 4. Children-specific legislation must be proactive and address design features over harm.

While prevention of harm is of utmost importance generally, the stakes of neglecting to mitigate risk before they materialize into harm is especially high for children given "both their developmental vulnerabilities and their status as 'early adopters' of emerging technologies." Without special consideration for children, Canada's current plans to address harmful content online flatten impact from known harms across groups that are differentially and disproportionately affected by the digital environment.

Recent evidence shows social media companies such as Facebook are already aware of how their services harm children and young people, especially to their mental-health and psychological wellbeing. The same companies are well resourced and adept at implementing proactive measures to safeguard specific threats, such as those to national security. Yet Canada's proposal to address harmful content includes minimal accountability mechanisms for mitigating risks to children before they become harms. As many have noted, the amplification of online content means that even the most violent and dangerous material can reach millions of children before it is flagged and removed.

One way to ensure proactive mitigation of harm outside controversial provisions to monitor all harmful content through automated filtering currently included in Canada's proposal is by incorporating clear instructions for the **design** and **testing** of services before they are deployed (or modified). Such systematic approaches, incorporated in the European Union's recently unveiled <u>Digital Services Act</u> and the aforementioned Age-Appropriate Design Code in the United Kingdom, are already showing promise in affecting change. In the weeks leading up to the passage of the latter specifically, a number of major platform companies including Instagram, YouTube, TikTok and Google

introduced changes to how they treat child users on their platforms. Instagram for instance, will no longer allow unknown adults to send direct messages to children under 18, while Google will stop targeted advertising to children under 18.

Lastly, incorporating age-appropriate design standards and proactive measures moves legislation beyond a narrow focus on harm and allows policymakers to support children and youth's autonomy and growth in online environments by maximizing their benefits and embedding children's rights by default and into design. As leading children's rights organization <u>5Rights</u> argues, "The enormous potential of digital technology will only be realised when it is proactively directed towards the promotion of children and young people's rights, rather than retroactively adapted or deployed merely to protect their safety.

We echo the need for Canada to introduce legislation to address online harms. As many have highlighted however, significant nuance and consultation is needed to ensure Canada gets it right. If the federal government takes this time now to consider special categories for the scope and definition of harmful content likely to be encountered by children, and protect both individual and collective children's rights with proactive measures (beyond automated filtering), it can very well lead the way in international norm setting.

han start ford a character film (francés) sa an teor le se anna a start a start film (francés) le se angla agusta a start a start a start a start le se start a start a start a start a start a start a start le se start a start a start a start a start a start

September 27, 2021

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St Gatineau QC K1A 0S5

Submitted via email: pch.icn-dci.pch@canada.ca

Dear Representatives of the Digital Citizen Initiative,

The Alliance for Safe Online Pharmacies Canada (ASOP Canada) is pleased to participate in the Government of Canada's consultation on harmful content online. As more Canadians rely on the internet for social, business, and information sharing, especially during and post-pandemic, we believe that there is a need for the public health and public safety of Canadians to be protected through a regulatory framework and appropriate resources that address the current usage and abuse/harmful content found online to create a safe environment for Canadians.

ASOP Canada is a project of ASOP Global, a global non-profit organization dedicated to keeping the public safe from illegal online sellers of prescription medicines and protecting the integrity of our legitimate pharmaceutical supply chain. We have a diverse membership that includes pharmacists, pharmacies, distributors, and our observers include the National Association of Pharmacy Regulatory Authorities (NAPRA), Healthcare Excellence Canada, GS1 Canada, among others. ASOP Canada works with local and international law enforcement, government, academics, and victim organizations to identify the threats of illegal online content and the appropriate tools to tackle illegal online content.

ASOP Canada is encouraged by the Government of Canada's progress to tackle online harm through proposed legislation and regulation; however, there is an opportunity being missed by the Government with the exclusion of illegal online sales of drugs, including opioids, in the proposed legislation and regulatory framework. The growing accessibility of illicit opioid sales online amidst Canada's opioid crisis requires the inclusion of opioid sales in the proposed approach to tackling online harm to reflect the current challenges faced online, especially the challenges directly related to youth safety in Canada.

#### Online Sale of Illegal Drugs

The illegal online sale of counterfeit medicine is not new. Criminal actors have long used social media and the online market to sell controlled substances, including opioids, other prescription medications and medicinal cannabis, through unlicensed sites, causing harm through inappropriate use or selling counterfeit drugs. These same criminal networks have now moved into the space of COVID-19, preying upon the uncertainty and fear of the public to sell one of the most globally sought-after products, COVID-19 vaccines. Pharmaceutical crimes are an increasing global issue; a record number of fake online pharmacies were taken down during Operation Pangea XIV, targeting the sale of counterfeit and illicit medicines and medical products. This year's operation resulted in 113,020 web links, including websites

and online marketplaces being shut down or removed, the highest number since the first Operation Pangea in 2008.<sup>1</sup> This increase demonstrates the ability for criminal networks to respond and adapt to changing environments and the need for enforcement agencies to adjust and work with partners to disrupt their activities.

The COVID-19 pandemic has also contributed to the worsening overdose crisis, with <u>some communities</u> reporting record-high numbers of overdose deaths, hospitalizations, and emergency medical service calls.<sup>2</sup> Without appropriate measures to stop these criminal networks, they will apply their successes in preying on Canadians for a profit and apply these techniques to the next opportunity. The online sale of opioids evolved along with the expansion of the internet, with sales moving from website forums to search engine results, and now social media sites such as Facebook, Twitter, Instagram, and LinkedIn.<sup>3</sup> This expansion demonstrates the criminal network's ability to infiltrate the internet, requiring a regulatory and enforcement framework to identify and address threats in this evolving environment.

The United States has taken a leadership role in tackling the online sale of opioids through the Food and Drug Administration's annual <u>Online Opioid Summit</u>, where stakeholders from prominent search engines, social media platforms, domain name registries and registrars, online marketplaces; advocacy groups, other government agencies, and academic researchers with expertise in this topic discuss **"ways to collaboratively take stronger action in combatting the opioid crisis by reducing the availability of illicit opioids online."**<sup>4</sup>

Additionally, the United States Department of Health and Human Services is finding new ways to take down the criminal networks involved in the illegal online sale of opioids by investing in an <u>artificial intelligence-based tool</u> to track how online opioid sellers and illegal internet pharmacies market and sell opioids. The tool will address law enforcement's issue whereby **only a small percentage of social media posts that mention opioids are related to illegal selling or marketing**. In one study of more than 600,000 tweets containing the names of several prescription opioids, it was found that fewer than 2,000 tweets were identified as actually marketing those substances.<sup>5</sup> Another issue is that drug dealers use evolving strategies and keywords to post illegal medications – making it difficult to track and take down posts with a simple keyword search. To address these issues, the tool will use Al focused on recognizing patterns in data so the system can recognize what drug-selling content looks like and find new posts across broader internet and social media platforms. While the leadership of the United States in the area of combatting online opioids takes more opioids off the internet, without the appropriate regulatory framework and resources, it also makes Canada a safe haven for criminals to operate.

infobase.canada.ca/substance-related-harms/opioids-stimulant

<sup>&</sup>lt;sup>1</sup> INTERPOL. Press Release: Thousands of fake online pharmacies shut down in INTERPOL operation (June 8, 2021). https://www.interpol.int/en/News-and-Events/News/2021/Thousands-of-fake-online-pharmacies-shut-down-in-INTERPOLoperation

<sup>&</sup>lt;sup>2</sup> Health Canada. Opioid- and Stimulant-related Harms in Canada Published:(June 2021). <u>https://health-</u>

<sup>&</sup>lt;sup>3</sup> Mackey, Tim. Opioids and the Internet: Convergence of Technology and Policy to Address the Illicit Online Sales of Opioids. Health Services Insights V.11 (2018).

https://www.researchgate.net/publication/327647893 Opioids and the Internet Convergence of Technology and Policy ( o Address the Illicit Online Sales of Opioids

<sup>&</sup>lt;sup>4</sup> United States Food and Drug Administration. News Release: Online Opioid Summits. <u>https://www.fda.gov/drugs/news-events-human-drugs/online-opioid-summits</u>

<sup>&</sup>lt;sup>5</sup> Mackey TK, Kalyanam J, Katsuki T, Lanckriet G. *Twitter-Based Detection of Illegal Online Sale of Prescription Opioid*. Am J Public Health. 2017 Dec;107(12):1910-1915. <u>https://pubmed.ncbi.nlm.nih.gov/29048960/</u>

han sharkan eestaa kelaa keesa saraba keesa aha aha Meriy Daharan kaa 2000 ahaa keesha ahaa dahaa ahaa aha dheriheesha ahaa ahaa kaada saraba

#### Multilateral Cooperation

In a recent issue briefing by the United States Congress <u>United States-China Economic and Security</u> <u>Review Commission</u>, there was a call for multilateral cooperation, particularly when addressing the presence and supply chain of illicit fentanyl in North America. As the United States Drug Enforcement Administration outlined in its <u>2020 National Drug Threat Assessment</u> report, China was identified as a primary source of "the primary source of fentanyl and fentanyl-related substances trafficked through international mail and express consignment operations, as well as the main source for all fentanylrelated substances trafficked into the United States."<sup>6</sup> This comes after China's government banned the production and sale of fentanyl and several of its variants in May 2019. However, according to a <u>National Public Radio (NPR) investigation and research from the Center for Advanced Defense Studies</u>, Chinese vendors have moved to online platforms to market and ship fentanyl and precursor chemicals used to make fentanyl directly to customers using postal delivery in the United States, Canada, and Europe. The Commission's report stated that the fentanyl being found in the United States can also be found in Canada as "China remains a primary source of illicit fentanyl in Canada, where opioid usage has increased since the start of the COVID-19 pandemic."<sup>7</sup>

During the May 26<sup>th</sup>, 2021, <u>Steering Committee meeting of the Canada-United States Joint Action Plan</u> on Opioids 2021, participants identified the following activities to improve North American capacities and collaboration and help Canada and the United States tackle the opioid epidemic in North America.

- Law Enforcement: expand measures to share intelligence to better understand cross-border drug trafficking, make investigations more effective, and disrupt domestic manufacturing of illegal synthetic opioids in Canada and the United States.
- Border Security: pursue opportunities to share resources and strengthen the capacity of border services personnel to detect and interdict fentanyl, its related substances, and other synthetic opioids illegally crossing our borders.
- Postal Security: formalize Canada-United States coordination to target opioids and other illegal drugs shipped through the mail; hold joint training sessions and regular meetings to share information, best practices, and improve our capacities to address this challenge.
- Health: share best practices and approaches to surveillance and applied research evaluating the impacts of COVID-19 measures on the opioid overdose crisis.<sup>8</sup>

An issue that arises in Canada's ability to appropriately participate in the multilateral cooperation to address the illegal supply of opioids is the gap in the data of the scope of the online opioid market. As there are definite trends in the presence of social media, web marketing, and purchasing of illegal opioids through seizures by law enforcement and border and postal services, there is no central tracking and tracing of the sources of these transactions (i.e. direct to consumer / criminal networks, online/social

https://www.dea.gov/sites/default/files/2021-02/DIR-

<sup>&</sup>lt;sup>6</sup> U.S. Drug Enforcement Administration, 2020 National Drug Threat Assessment, March 2021.

<sup>00821%202020%20</sup>National%20Drug%20Threat%20Assessment\_WEB.pdf.

<sup>&</sup>lt;sup>7</sup> United States Congress: U.S.-China Economic and Security Review Commission. Illicit Fentanyl from China: An Evolving Global Operation, August 24, 2021. <u>https://www.uscc.gov/sites/default/files/2021-08/Illicit Fentanyl from China-</u> An Evolving Global Operation.pdf

<sup>&</sup>lt;sup>a</sup> Public Safety Canada. Steering Committee meeting of the Canada-U.S. Joint Action Plan on Opioids 2021. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-int-ctn-pds/index-en.aspx.

media/ street purchases) which impedes on the ability for the government, law enforcement, and multilateral groups to identify the appropriate solutions to address the opioid epidemic.

#### **Online Harm Discussion Paper**

The discussion and technical paper released by Heritage Canada addresses the known dangers that have come with the widespread use and growing number of online platforms. While social media platforms and online services enable families and friends to connect and share content, these platforms have also become breeding grounds for individuals to spread hate, enable dangerous groups and networks to incite violence and perpetuate harmful content to children.

The proposed framework appreciates the evolution of technology and everchanging social habits of Canadians; however, the application overlooks fundamental areas of concern that must be addressed. The content targeted by the new legislation is based on actions that are already considered illegal; however, the five categories must be more comprehensive to promote a safe and non-violent online space, especially for children.

The discussion guide released by Heritage Canada recognizes that social media companies are reactive in nature and are not required to preserve evidence of criminal content or notify law enforcement about criminal content (except for child pornography, where they are required to report). However, with this in mind, the harmful content addressed by the legislation can be broader and should reflect the current, ongoing challenges faced online, especially the challenges directly related to youth safety in Canada.

#### Recommendation:

Illicit online opioid sales should be included as a targeted category of harmful content under Canada's proposed online harm legislation. The growing accessibility of illicit opioid sales online, coupled with Canada's pressing opioid crisis, justifies the inclusion of opioid sales within the harmful content definition. Furthermore, opioid sales have been included within international definitions for content abuse.

As indicated below, the illegal distribution of opioids online is included in the definition of content abuse, in addition to human trafficking, child sexual abuse, and incitements to violence as grounds to take action to remove or block the content. We recommend that both Canada's regulatory framework and intermediaries adopt the following definition for online harm.

When Should a Registrar or Registry Act on Website Content Abuse? Despite the fact that registrars and registries have only one blunt and disproportionate tool to address Website Content Abuse, we believe there are certain forms of Website Content Abuse that are so egregious that a registry or registrar should act when provided with specific and credible notice. Specifically, even without a court order, we believe a registry or registrar should act to disrupt the following forms of Website Content Abuse: (1) child sexual abuse materials ("CSAM"); (2) illegal distribution of opioids online; (3) human trafficking;10 and (4) specific and credible incitements to violence. Underlying these Website Content Abuses is the physical and often irreversible threat to human life. Additionally, each registrar and registry has its own acceptable use policies or terms of use that set forth provisions that may cover these and additional forms of Website Content Abuses.<sup>9</sup>

<sup>&</sup>lt;sup>9</sup> The Government of Canada has an opportunity to align with international industry standards of the DNS Framework. The DNS Framework is an agreed upon code of conduct signed by 48 leading domain name registrars that outlines the roles and

By including a broader definition of online harm, Canada will be aligning with agreed-upon industry standards and reflecting the current landscape of online harm that Canadians are subject to.

#### **Telecommunications Service Providers Exemption**

Online harms are often present in private messaging; however, the legislation would not cover private communications or telecommunications service providers (such as WhatsApp). The language provided at Module 1(D) at paragraph 120 would apply to telecommunication services providers in exceptional circumstances. The Telecommunications Act at s. Thirty-six states that ... "except where the Commission approved otherwise, a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public"; therefore, it would be challenging to enforce content that is shared in any capacity through a private telecommunication service. As technology evolves, many telecommunication service providers \*also\* include social media capabilities, and this area must be explored as technology evolves.

#### **Consultation on Modules**

Module 1(A), paragraphs 6-8 of the Technical Paper provides: the Act, including any statutory and regulatory obligation imposed on OCSPs, should apply with respect to the five (5) types of harmful content described below:

The concept of child sexual exploitation content should capture 1) criminal law offences in this area set out in the Criminal Code, in a manner adapted to a regulatory context, including child pornography and other sexual offences relating to children; and 2) material relating to child sexual exploitation activities that may not constitute a criminal offence, but when posted on an OCS is still harmful to children and victims (e.g., screenshots of videos that do not include the criminal activity but refer to it obliquely; up-to-date photos of adults who were exploited/ abused as children being posted in the context of their exploitation and abuse as children).

#### Recommendation:

The Act must be more inclusive in terms of content and materials directly correlated to children and child exploitation. Online child sexual exploitation is one of the most disturbing public safety issues facing society today<sup>1</sup>. The proposed legislation must be more inclusive in detailing the content that would fall under this concept.

Canada has seen a rise in child exploitation cases that also involve drugs. The cases below demonstrate the recent increase in online child exploitation/luring investigations that led to further charges related to the possession and/or distribution of drugs:

- Info from German police leads to child porn, drug charges in London, Ont. (May 2021)
- Police lay charges in child pornography and drug trafficking investigations (June 2021)
- Child luring investigation leads to drug and child porn charges in Chatham-Kent (March 2021)

Note: The National Child Exploitation Crime Centre (NCECC) and the provincial Internet Child Exploitation Units are excellent resources with respect to investigations related to the sexual exploitation of children on the internet in

responsibilities of domain name registrars to address online company creates, operates and can enforce requirements for domain extensions such as .ca, .com, .edu, .org, and .tech. Examples of registries include Canadian Internet Registry Authority (CIRA), Verisign, Radix, Neustar, etc. A domain name registrar is an accredited company that sells domain names to the public. Examples of registrars include Rebel and Tucows (Canada-based), and GoDaddy.harm. A domain name registry (DNR)

Canada. In the proposed amendments to the Mandatory Reporting Act, the government would centralize mandatory reporting of online child pornography offences through the NCECC.

The examples above demonstrate the link between the sexual exploitation of children, child pornography and **drug offences**.

The concept of content that involves promoting and distributing drugs is non-existent in the current proposed legislation. Suppose the goal is to make Online Communication Services and Online Communication Service Providers more accountable and transparent in combatting harmful online content. In that case, we cannot exclude a category that has an enormous impact on the safety of Canadians, especially youth. By way of example, the opioid overdose crisis in Canada is alarming, that is a well-known, challenging fact. Additionally, this legislation is being discussed and implemented amid a global pandemic. The effects of COVID-19 on youth and the risks associated with mental health issues and growing substance abuse are significant at the moment.<sup>1</sup> Canadians have never spent this much time online, and bad actors will capitalize on the current climate and target vulnerable groups to further their motives.

#### Module 1(B), paragraph 30 reads: The Act should provide that **nothing in the Act requires or authorizes** an OCSP to proactively seek out illegal content <u>outside of the five (5)</u> categories of regulated harmful content.

#### Recommendation:

When considering the platforms that this new legislation would impact, many already have community guidelines and policies in place which prohibit attempts by individuals, manufacturers, and retailers to *purchase, sell or trade non-medical drugs, pharmaceutical drugs.* Though many platforms already use technology and algorithms to detect (and enforce) prohibited and illegal content, more thought and consideration of the categories included in the legislation must occur. We should be complimenting the protocols already in place for specific information and content – not limiting it to a box of definite categories.

Moreover, child exploitation is not just sexual exploitation; different types of exploitation include, and are not limited to, labour exploitation and domestic servitude. There must be an avenue for OCSs and OSCPs to seek out this type of content and activity online, especially as it applies to youth, and be able to apply all necessary policies and procedures in their efforts to remove and punish individuals responsible. We recognize the complexity and comprehensive nature of combatting online harm. We encourage the Government of Canada to continue discussions with law enforcement, academics, and industry to ensure that Canada's regulatory framework addresses the public health and public safety threat of the online sale of illegal and illicit drugs, including opioids.

We welcome any questions or requests for further briefings on the issues and recommendations outlined above.

Sincerely,

Dani Peters

Dani Peters, Advisor ASOP Canada dani.peters@buysaferx.pharmacy Digital Citizen Initiative Department of Canadian Heritage September 25<sup>th</sup>, 2021

#### **Proposed Legislative changes and Regulatory Bodies**

For the purpose of this submission, I represent the BC Coalition of Experiential Communities;

The **BC Coalition of Experiential Communities** are a consortium of sex workers who are activists mandated as a mechanism for the voices of experiential people to support the development of legislation and policies; peer driven programs and services; and work toward the elimination of oppressive systems and forces that create harm within the sex industry.

1 am writing today to express the reasons why adult entertainers/ sex workers must be included in any actions, proposed legislative changes and "advisory bodies" which will govern the proposed regulation of on-line content.

Sex workers are the experts on our lives and safety. Any legislation which could impact the lives and safety of sex workers in Canada must include our voices and perspective.

#### Canadian Human Rights Act

#### The General Assembly,

Proclaims this Universal Declaration of Human Rights as a common standard of achievement for all peoples and all nations, to the end that **every individual and every organ of society**, keeping this Declaration constantly in mind, shall strive by teaching and education to promote respect for these rights and freedoms and by progressive measures, national and international, to secure their universal and effective recognition and observance, both among the peoples of Member States themselves and among the peoples of territories under their jurisdiction.

Sex Workers note that the UN Charter of Human Rights addresses a broader cross section of society and works to include all people who experience discrimination. The Canadian Charter does not go as far and excludes key phrases and wording which prevent sex workers from holding to account those people who violate our human rights with complacency in an on-going way.

#### Article 2

Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or **other status**. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.

If the government is revising the Canadian Human Rights Act, Sex workers and our community respectfully request that this detail - "*other status*" - is added to Canadian legislation to better reflect the original spirit of the UN Charter.

Sex workers regularly experience hate crimes and discrimination.

Bushby, then 18, was a passenger in the vehicle driving along McKenzie Street on the city's south side during the early morning of Jan. 29, 2017. Bushby, who was drinking heavily, had said he wanted to drive around and yell at sex-trade workers.

#### https://www.cbc.ca/news/canada/thunder-bay/brayden-bushby-barbara-kentner-sentencing-1.6056010

While this prosecutor declared this was a hate crime against women, it was actually a more specific targeting of an easily identifiable and discriminated against group, sex workers.

He knew he could get away with driving around harassing and being violent towards sex workers. He knew that no one cared about a sector of society cast by the government and Canadians as "less than", "dirty" or "disposable".

Even the sentence he received reflects the hatred of sex workers in society more broadly. If he had killed anyone else, he would have received life in prison.

Any discussions about sex work in the public sphere are rife with falsehoods, ideology and morally based arguments which have no place in discussions about the lives and safety of Canadian citizens, PEOPLE.

The rhetoric which is always loudest and front and center in any conversations about sex work have created this perception of sex workers as damaged, reasonable casualties in the war on "trafficking" and as an evil needing to be "removed" from society.

When we discuss adult film/ pornography it is NOT some megalithic "thing" to be hated and destroyed. It is people, working to feed and house themselves and their families.

Violent and targeted terrorist attacks on sex workers in their work places in Atlanta and Toronto demonstrate this hatred of sex workers and the ways in which this hatred, promoted by those wishing to abolish our community and by the Canadian Government, plays out in real world acts of violence. This violence is not theoretical, it is real and predictable.

https://www.cbc.ca/news/canada/toronto/incel-terrorism-massage-parlour-1.5575689

https://www.cnn.com/2021/03/16/us/metro-atlanta-spa-shootings-what-we-know/index.html

Since the Canadian Human Rights Act is already being revised to accommodate the new approaches being proposed here, Sex workers request;

- The addition of "occupation" or "other status" to Section 2 of the Act Purpose.
- The addition of "occupation" or "other status" to all provisions of the Act to ensure people working in sex work or adult entertainment more broadly do not face discrimination in any of the ways detailed in the Act.
- That all relevant systems of complaint are given guidance on how the Act protects sex workers and adult entertainers from discrimination and how to apply that new protection under the charter as a separate and distinct group often targeted for violence, terrorism and hatred as a result of their occupational status.

Our community deserve the same protections as other easily identifiable groups. We deserve to be protected from violence, terrorism, discrimination and hatred in all the ways outlined in the Act.

The government have already opened the act for revision, now is the time for that recognition and inclusion as targets of violence, terrorism, hatred and discrimination who qualify as distinct and easily identifiable group.

#### **Establishment of new Regulators**

Canadians agree that the current "wild west" status of the internet causes problems on many levels and that some form of regulation is required in order to protect people from all of the harms outlined in the proposed processes.

However, nowhere in the proposed mechanisms are sex workers or adult entertainers mentioned.

Given that a minimum of 100,000 (up to approx. 250,000) Canadians rely on adult entertainment as their sole source of income to feed and house themselves and their families, consideration must be given to the perspectives and experiences of these workers and legal industry.

The adult entertainment community of workers and entrepreneurs are asking for the following additions and changes to the framework as outlined in both the Discussion document and Technical document;

#### Module 1(a) - New Legislative and Regulatory Framework

- Recognize that OCS is used by more than 100,000 Canadians as their sole means of income in the legal adult entertainment sector.
- Addition to (c) Consider that the hatred spread online often has a disproportionate impact on women, Indigenous Peoples, members of racialized and religious minority communities and on LGBTQ2 and gender-diverse communities, persons with disabilities and people working in the adult entertainment sector;

#### Application

- The Act should include definitions of content which is NOT harmful to ensure that legal work in the adult entertainment sector is not impacted by ideological opinions and efforts to counter exploitation or "end the sex industry".
- Specific definitions to ensure that this safe, legal employment sector is not undermined by hateful expressions of myths about sex workers lives. That truth about sex work and adult entertainment, ethical research which meets the test of the Tr-Council Policy Statement (2) are only used to inform any actions taken to counter exploitation in the adult sector.
- The Act should specifically state that impartiality is a critical feature of any regulation of the adult sector and that sweeping statements, based in hatred, are not entertained or allowed to influence any regulation of or enforcement against this legal employment sector.

#### Module 1(B): New Rules and Obligations

- General Obligations 10(a) The Act should provide that an OCSP must take measures to ensure that the implementation and operation of the procedures, practices, rules and systems, including any automated decision making, put in place for the purpose of moderating harmful content that is communicated on its OCS and that is accessible to persons in Canada, do not result in differential treatment of any group, *including adult entertainers and sex workers*, based on a prohibited ground of discrimination within the meaning of the <u>Canadian Human Rights Act</u> and in accordance with regulations. *(this addition needs to be specifically added so as to prevent misuse of rules by anti sex work zealots)*
- 14. The Act should provide that an OCSP must generate and provide reports on a scheduled basis to the Digital Safety Commissioner on Canada-specific data about:

 (f) – How they monetize harmful content – should read "how they monetize content" - harmful content assumes the OCSP is purposely monetizing harmful content and reflects an inherent bias from the onset of this proposed regulatory body.

#### Incident response protocol

18. [D] The Act should provide the Digital Safety Commissioner with the authority, with the approval of the Governor in Council, to establish an Incident Response Protocol for the purpose of implementing the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online and reducing the online communication of content relating to terrorist activities. The Incident Response Protocol would respond to an act or omission as described in the definition of "terrorist content" tied to an emergent, ongoing, or recently concluded real-world attack in Canada, or outside of Canada when content is shared on one or more Canadian-based OCSs.

Sex workers and adult entertainers would like to point out that the attacks in Toronto and Atlanta against massage parlor workers would qualify under this provision. This would require the removal of hateful/untrue/malicious content by anti sex work organizations and which has lead directly real world acts of violence and terror against the Canadian sex working community.

Content created by those groups actively promoting hatred of sex workers and the abolition of our community is widely available in Canada. After an attack like the Toronto attack, we would hope to see those OCSP who host this kind of hateful content held to account and that content removed.

We would also hope to see any funding of these individuals and organizations via public money stopped in respect of the inherent threat they pose to the sex working community in Canada.

#### Module 1(C): Establishment of the new regulators

#### Digital Safety Commissioner

#### **Establishment and Function**

35. The Act should provide for the establishment of the Digital Safety Commissioner, whose functions are to:

(a) Oversee and improve online content moderation, by:

1. Administering and enforcing obligations;

Ensuring balanced and unbiased consideration of complaints about the legal adult entertainment sector and which reflects an understanding of the negative impacts actions taken may have on the lives and safety of Canadians working in adult entertainment and their families.

2. Engaging with and considering the particular needs of and barriers faced by groups disproportionately affected by harmful online content such as women and girls, Indigenous Peoples, members of racialized communities and religious minorities and of LGBTQ2 and gender-diverse communities, persons with disabilities and **people working in sex work or the adult entertainment sector**; and

2. Supporting platforms in reducing harmful content affecting peoples in Canada.

#### Composition

0

- 38. The Act should provide that a person appointed as Commissioner or Deputy Commissioner must declare any conflict of interest, *in particular any history of a private interest in the abolition of the sex industry*, and must not be a shareholder of an OCS or OCSP.
- Digital Recourse Council of Canada

#### Composition

46. The Act should provide that the Digital Recourse Council of Canada will be composed of no fewer than three (3) and no more than five (5) members, appointed by the Governor in Council. The Governor in Council will designate one (1) member as the Chairperson and may designate one (1) member as the Vice-Chairperson. The Act should provide that in appointing members, the Governor in Council shall take into consideration the importance of diverse subject-matter experts reflective of the Canadian population, particularly inclusive of women, Indigenous Peoples, members of racialized communities and religious minorities, of LGBTQ2 and gender-diverse communities, persons with disabilities and *sex workers*.

Sex workers note that the proposed limit of commission members is 5 but the stakeholder groups number 8. This is a fundamental flaw with the proposed Commission and the number of members should reflect the number of groups identified by the government and sex industry representatives.

48. The Act should provide that the Digital Recourse Council of Canada's members must declare any conflict of interest, *including a private interest in the abolition of the sex industry*, and must not be a shareholder of an OCS or OCSP.

Sex workers know that those people who promote hatred of our community are lining up to be appointed to this committee/ council which will have power over our lives and safety. Any person who holds a private interest in the abolition of the sex industry must NOT be granted a position on the Council. It is a conflict of interest and has inherent tangible value to those who base their income and power on the oppression of the sex industry community via promotion of hatred, bias assertions and the ideology of all sex work being violence

Adult Entertainment and adult film work are legal in this country and represent a large percentage of people employed via use of OCSP. Any actions proposed which could undermine our lives, safety, ability to feed and house ourselves and our families must consider those impacts and seek feedback/ input from our community before being adopted.

The legal adult entertainment sector must have a place on this Council and be recognized as critical to the success of it's stated goals.

#### Advisory board

71. The Act should provide for the establishment of an Advisory Board composed of no more than seven (7) members who are appointed by the Minister at pleasure. The Act

should provide that the Minister consider the importance of inclusive membership of the Advisory Board reflective of the Canadian population, particularly inclusive of women, Indigenous Peoples, members of racialized communities and religious minorities, of LGBTQ2 and gender-diverse communities, persons with disabilities **and sex workers**.

72. The Act should provide that in appointing members, the Minister take into consideration the importance of having members that are knowledgeable about or have experience related to law, technology, equity and social science, and are drawn from advocacy groups, including civil liberties, equity or victim advocacy organizations, the online communication industry, *adult entertainment workers* and academia.

#### Conclusion

Canadian Adult entertainers have been disproportionately impacted by the pandemic and many have turned to OCPS to feed and house themselves and their families via legal income. From the beginning the adult industry has had a large presence on the internet and has provided safer work options for sex working people in Canada.

Any regulation or regulator being created must include representatives from this legal industry and ensure that ideological opinions and goals of a few anti sex industry zealots do not undermine the human rights of Canadians who work or are entrepreneurs in this sector.

Those people who hold a private interest in the abolition of the sex industry must NOT be given power over our lives and safety. They have proven time and time again to know no depths when it comes to achieving those personal private interests and have no ethics in how they reach those goals.

This Submission outlining some of the issues with the proposed regulatory framework only begins to highlight the glaring omissions of these provisions and proposed mechanisms.

The potential for biased and dangerous actions against the sex industry community are predictable and overt.

The only solution is sex industry representation and inclusion in both the Canadian Human Rights Act and the development of the regulatory processes being outlined here.

I will remind the reader that as public servants, you have sworn an oath of office. That oath binds you to impartiality and preventing the appearance of a conflict of interest. I have seen 4 different Codes of Conduct which govern work in the Public Sector and require the sex industry is represented/ included and that hate crimes/ hate speech against our community is addressed. The rules governing Conflict of Interest also demand that those groups and individuals who hold a private interest in the abolition of the sex industry must not be given power over our lives and safety.

I am available at any time to discuss these issues and how Canada can respect the rights and safety of all citizens in this work to address harmful content on the internet in particular as it relates to terrorism against and promotion of hatred of my community, sex workers.

Susan Davis Director BC Coalition of Experiential Communities 604-671-2345 www.bccec.wordpress.com

Goournent communique ou vient de la Lin aux innoès à l'Information Document rulessoit purcuent lo Ille Access la minimizion - ci

# Response to 'The Government's proposed approach to address harmful content online'

Submitted to the Digital Citizen Initiative at the Department of Canadian Heritage

OpenMedia is a community-based organization that safeguards the possibilities of the open Internet.

September 25, 2021



# media

Instantion constant the second

### OVERVIEW OF RESPONSE

A. Introduction	2
i) About OpenMedia	2
ii) Context of the consultation	2
iii) This consultation is not adequate or legitimate	3
B. Concerns on the proposed legislative remedies	5
i) Go fast and break things: 24-hr takedowns guarantee over-policing of content	5
ii) Content moderation will never be completely unbiased	8
iii) Proactive surveillance obligations are unfit for democratic use	8
iv) Direct reporting to law enforcement treats all Internet users as criminals	9
v) Website blocking is disproportionate, ineffective, and unwelcome in Canada	11
vi) Legal remedies must use the court system	12
vii) An all-powerful regulator is not the answer	13
viii) The proposal will harm those it claims to help	14
ix) Setting a dangerous precedent with global ramifications	15
C. What a better discussion of online harms might look like	16
i) Clearly separate illegal content from online harms	16
ii) Addressing the knowledge gap around harmful online content	17
iii) Empowering internet users; not Big Tech	19
D. Conclusion	22

OpenMedia is a community-based organization that safeguards the possibilities of the open Internet.

# A. Introduction

#### () About OpenMedia

OpenMedia is a community-driven organization of over 350,000 members that work together to keep the Internet open, affordable, and surveillance-free. We operate as a civic engagement platform to educate, engage, and empower Internet users to advance digital rights around the world.

Our organization and community members have been active participants at the Canadian Radio-television and Telecommunications Commission (CRTC), and have participated in numerous parliamentary review processes and consultations on issues impacting Canada's digital policy. We work to connect those most impacted by policy decisions directly with those making those policies, expanding our democratic processes to maximize public engagement.

For this particular consultation, members of the OpenMedia community have already delivered more than 8,600 unique emails providing individual feedback to the Government of Canada's public consultation on harmful content online.

This formal response on behalf of the organization accompanies and reinforces our community members' individual messages, expanding on the concerns they've raised with the government about the plan for our Internet described in the consultation's discussion guide and technical paper.<sup>1 2</sup>

#### ii) Context of the consultation

OpenMedia recognizes this proposal appears to form part of a wider plan from the Canadian government to affect changes to Canada's Internet, covering both illegal content, and other behaviour and content that may be seen as harmful. Heritage Minister Steven Guilbeault has repeatedly spoken of rude speech against public officials as an online harm that is undermining democracy, and the Capitol insurrection in the U.S. as a product of uncontrolled online speech.<sup>3</sup> <sup>4</sup> The technical paper that accompanies this consultation itself frequently uses 'harmful content' as a stand-in for the five forms of illegal content it seeks to place new obligations on platforms to address, further muddying the issue.

We believe there are real problems with both illegal content on the Internet, and legal but in some ways harmful content. But as an organization whose mandate is to fiercely defend the

<sup>1</sup> Department of Canadian Heritage (2021). Discussion Guide

https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html <sup>2</sup> Department of Canadian Heritage (2021). *Technical Paper* 

Department of Canadian Hentage (2021). recrifical Paper

https://www.cbc.ca/news/politics/facebook-twitter-canada-regulation-1.5894301

<sup>4</sup> Canada 2020 (2021). Democracy in the Digital Age: Addressing Online Harms

https://canada2020.ca/democracy-in-the-digital-age-addressing-online-harms/

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC, Canada V5L 5G3 // 1-888-441-2640

https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html <sup>3</sup> Elizabeth Thompson (2021). "Canada not exempt from social media forces that created U.S. Capitol riot, heritage minister says." CBC January 29 2021.



legal expressive and privacy rights of people in Canada, the government's casual disregard for both of these rights is deeply concerning to us.

Minister Guilbeault has claimed that the government only seeks to "reproduce the same framework that exists in the physical world in the virtual world." <sup>5</sup> Yet the proposals within this consultation show a shocking lack of concern for maintaining this balance, or for understanding the real world impact they will have.

If adopted as written, the proposals in this consultation would lead directly and predictably to an unprecedented increase in the removal of considerable legitimate and lawful forms of speech online. It would also lead to the automatic reporting of an enormous volume of lawful content directly to the Royal Canadian Mounted Police (RCMP) and Canadian Security Intelligence Service (CSIS), deputizing online platforms as surveillance agents of the state in a system not seen anywhere else in the democratic world. And it would singularly fail to protect marginalized communities on the Internet, instead empowering their current victimizers in troll communities and law enforcement to more effectively target and harass them.

Policy-makers are responsible for the foreseeable consequences of their policies, not just their intended or desired outcomes. You are accountable for each of these disastrous consequences.

We're aware that other commentators are providing strong input to the consultation focused on the domestic legal and constitutional implications of the proposal, its compatibility with Canada's obligations under international law, and its potential incompatibility with the USMCA. We share their concerns, and note that a bill bearing striking similarities to the proposals in this consultation was recently struck down on constitutional grounds in France due to the precise issue of over-removal of lawful speech that we discuss below.<sup>6</sup>

Our submission will however focus on where we are best positioned to comment: an analysis of the predictable and damaging consequences of the proposal as described, (<u>Section B</u>), and a nudge towards more potentially more productive directions for future government intervention on these issues that should be explored instead (<u>Section C</u>).

iii) This consultation is not adequate or legitimate

The consultation presented to us does not have the features of a true public consultation, as has been pointed out by those both supportive and skeptical of new government regulation of

https://www.cbc.ca/news/politics/facebook-twitter-canada-regulation-1.5894301

<sup>6</sup> Conseil Constitutionnel (2020). *Décision n° 2020-801 DC du 18 juin 2020* https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC. Canada V5L 5G3 // 1-888-441-2640

<sup>&</sup>lt;sup>5</sup> Elizabeth Thompson (2021). "Canada not exempt from social media forces that created U.S. Capitol riot, heritage minister says." CBC January 29 2021.



Internet platforms.<sup>7 8</sup> This is nothing more than a formal presentation of a predetermined plan, with an unreasonably short time frame for public comment.

This consultation provides absolutely no opportunity to help shape the framework of either the problem at hand, nor any of the proposed solutions. Rather than a solicitation of public and expert input on what the government should do, the technical paper appears to be a list of what the government will do, regardless of what it hears during the consultation period. It asks no open-ended questions. It does not solicit any evidence about problems on online platforms, nor does it present any evidence that justifies or explains the systems it proposes. It does not entertain or even reference alternative or complementary approaches to its proposed measures.

This is unacceptable policy-making in a democratic society. But it is particularly egregious as the government considers infringing on our Charter of Rights and Freedoms, and limiting citizens' ability to participate in the primary public spaces of our era, online platforms.

The timing of this consultation is also deeply inappropriate. The deadline for public comment was never published on the consultation page, and the consultation period given in the announcement was too short for substantive public input. But once a federal election was called, this entire consultation should have immediately been rescheduled. This would have comported with Privy Council Office guidance for election periods, as the matters under consideration are very clearly neither routine nor non-controversial.<sup>9</sup>

The overlap with the federal election made public engagement with the consultation significantly more difficult, in part due to regulations placed on third parties in an election, in 2019's Bill C-76. It was further challenged by the limited capacity of experts, academics, public interest groups, and concerned citizens to speak out and mobilize the general public during an election period, and a time-bound requirement for election participation that distracted from the potential to simultaneously participate in this consultation. OpenMedia strongly suspects that the timing of this consultation has significantly reduced the amount of participation from subject matter experts, whose voices are critical in ensuring a fulsome discussion of such issues and proposals.

The consultation's irregularities and deficiencies are major reasons it has drawn widespread criticism from a broad swath of both the academic content moderation-focused community, and

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC, Canada V5L 5G3 // 1-888-441-2640

<sup>&</sup>lt;sup>7</sup> Haggart, Blayne and Tusikov, Natasha (2021). Not much of a consultation, not much of a plan: Our submission regarding the federal government's proposed approach to addressing harmful content online https://blaynehaggart.com/2021/09/24/not-much-of-a-consultation-not-much-of-a-plan-our-submission-reg arding-the-federal-governments-proposed-approach-to-addressing-harmful-content-online/

<sup>&</sup>lt;sup>®</sup> Internet Society Canada Chapter (2021). Submission to the Department of Canadian Heritage: Consultation on Online Harms

https://internetsociety.ca/wp-content/uploads/2021/09/ISCC-Response-Online-Harms-Final-21-9-21-1.pdf <sup>9</sup> OpenMedia (2021). Open letter: Defer consultations on the Internet until after the election https://openmedia.org/article/item/open-letter-reguesting-rescheduling-of-open-internet-consultations



the civil rights community, in Canada and abroad.<sup>10 11 12 13 14</sup> It compares very poorly to the more serious multi-year consultations that have been held in jurisdictions that have adopted broadly comparable legislation.<sup>15</sup>

Our participation in this consultation should not be read as acceptance or endorsement of this process. We strongly believe this consultation is utterly inappropriate. However, given the government's steadfast insistence on proceeding regardless, we feel we have no choice but to submit an insufficient submission, to ensure that at least some of our comments and concerns can be placed on the public record. If, as we recommend, the consultation is abandoned, it should be replaced by a much more fulsome public discussion about how best to encourage sound content moderation practices on Internet platforms.

Recommendation: The government should abandon this inadequate consultation, and the proposals contained within. Instead, it should pursue a genuinely open discussion on these issues, one that solicits evidence from all interested parties on the nature of problems with online content moderation and appropriate solutions that could be entertained to them.

## B. Concerns on the proposed legislative remedies

#### i) Go fast and break things: 24-hr takedowns guarantee over-policing of content

One of the key recommendations made by the consultation's technical paper is to implement a 24-hour timeline requirement for platforms to remove all potentially illegal content under the five categories identified: terrorist content, incitement to violence against people or property, hate

https://twitter.com/daphnehk/status/1421118036895961094

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC, Canada V5L 5G3 // 1-888-441-2640

<sup>&</sup>lt;sup>10</sup> Darryl Carmichael and Emily Laidlaw (2021). *The Federal Government's proposal to Address Online Harms: Explanation and Critique* 

https://ablawg.ca/2021/09/13/the-federal-governments-proposal-to-address-online-harms-explanation-and -critique/

<sup>&</sup>lt;sup>11</sup> Daphne Keller (2021). Twitter thread:

<sup>&</sup>lt;sup>12</sup> Lawbytes Podcast (2021). "Episode 99: Cynthia Khoo on the Canadian Government's Online Harms Consultation"

https://www.michaelgeist.ca/2021/08/law-bytes-podcast-episode-99/

<sup>&</sup>lt;sup>13</sup> Electronic Freedom Frontier (2021). O (No!) Canada: Fast-Moving Proposal Creates Filtering, Blocking and Reporting Rules—and Speech Police to Enforce Them

https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filtering-blocking-and-reporting-rules-1

<sup>&</sup>lt;sup>14</sup> Michael Geist (2021). *Picking Up Where Bill C-10 Left Off: The Canadian Government's Non-Consultation on Online Harms Legislation* 

https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/

<sup>&</sup>lt;sup>15</sup> Haggart, Blayne and Tusikov, Natasha (2021). Not much of a consultation, not much of a plan: Our submission regarding the federal government's proposed approach to addressing harmful content online https://blaynehaggart.com/2021/09/24/not-much-of-a-consultation-not-much-of-a-plan-our-submission-reg arding-the-federal-governments-proposed-approach-to-addressing-harmful-content-online/

#### OpenMedia is a community-based organization that safeguards the possibilities of the open Internet.

speech, non-consensual sharing of intimate images, and child sexual exploitation content. A harsh penalty of 3% of global revenue or \$10 million dollars would be applied to any platform that fails to meet the standard.<sup>16</sup> This requirement will be in effect from the time a platform becomes aware of the content – which could mean from when it is posted, or any time content is flagged or reported by any user.

The government has presented this as a way of getting 'tough' on platforms who are not doing enough to remove illegal content. But this view ignores the predictable consequences these requirements will have on platform behaviour, and the subsequent impact on Internet users. In practice, this obligation will lead directly and overwhelmingly to the removal of large amounts of user speech which would not be found illegal by a court of law. This problem is especially acute as much of the content being flagged will be identified by individual platform users who object to the content, but are not legal experts, and not necessarily able to identify the difference between what is illegal, objectionable, or just something they dislike.

Handling the volume of content moderation decisions required daily on a major online platform with any degree of fairness to users is extremely challenging.<sup>17</sup> Any content moderation system inevitably produces errors, whether using either human or algorithmic judgment. At present, platforms continually readjust their standards and systems to account for widely criticized mistakes in both failing to remove content, **and** inappropriately removing content.

The one-sided obligations imposed in this proposal will put a heavy thumb on the scale in favour of systematically over-removing lawful content. The platform incentives are clear: there will be a heavy legal and financial risk attached to leaving up content that could conceivably be found illegal under any of the five harms of this proposal, but no counter-balancing incentive to encourage thoughtful or fair consideration of the expressive rights of the posting user.

Put plainly, the inevitable outcome of this obligation will be the removal of all but the most obviously innocuous content flagged under these harms within the 24-hr window, regardless of its legitimacy.

This outcome thoroughly undermines the government's stated objective of merely translating our offline speech standards to the Internet. And it cannot and will not be remedied by appealing to the government's proposed Digital Recourse Council to reinstate content. Platforms have no obligation or clear incentive to ever reinstate content; and returning speech to a platform months or years after it was posted is not meaningfully equivalent to allowing it in the first place. Further, studies have shown that having any content removed has a demonstrated chilling effect on

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC. Canada V5L 5G3 // 1-888-441-2640

6

media

<sup>&</sup>lt;sup>16</sup> Department of Canadian Heritage (2021). Technical Paper Para. 11(A), 108[J].

https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html <sup>17</sup> Michael Masnick (2021). Masnick's Impossibility Theorem: Content Moderation At Scale Is Impossible

To Do Well.

https://www.techdirt.com/articles/20191111/23032743367/masnicks-impossibility-theorem-content-moderation-scale-is-impossible-to-do-well.shtml



further speech, both of the affected user and those who see their content removed, directly discouraging participation in public conversation.<sup>18</sup> <sup>19</sup>

A very wide range of lawful user speech could potentially fall afoul of the necessarily broad interpretation platforms will make of what could constitute illegal content, including but most certainly not limited to:

- Satire and humour;
- Support for or participation in protest movements;
- Documentation of human rights abuses;
- Artistic expression;
- · Research and journalism on sensitive or violent topics;
- Voluntary adult sexual expression;
- · Conversation by or within marginalized communities about their lived experience.

This potential mistargeting of lawful and important user speech is not hypothetical. Currently, platforms' content moderation that is intended to protect against hate speech frequently leads to unintended censorship of targeted groups.<sup>20 21</sup> Similarly, attempts to remove content that glorifies violence frequently misfire and censor critical reporting and documentation of real world atrocities.<sup>22 23</sup> Pressure from states has even platforms to directly interfere in critical, lawful social discourse about the justice and legality of government actions.<sup>24</sup>

A more thoughtful assessment of current online platform takedowns of illegal content should examine the average time verified illegal content remains online, and the reasons why, which

https://citizensandtech.org/2020/09/chilling-effect-automated-law-enforcemen/

<sup>20</sup> Conor Murray (2021). "TikTok algorithm error sparks allegations of racial bias." NBC July 9 2021.

https://www.nbcnews.com/news/us-news/tiktok-algorithm-prevents-user-declaring-support-black-lives-mat ter-n1273413

https://www.nytimes.com/2017/08/22/world/middleeast/syria-youtube-videos-isis.html

<sup>&</sup>lt;sup>18</sup> Jonathan Penny (2017). "Internet surveillance, regulation, and chilling effects online: a comparative study", *Internet Policy Review* Volume 6:2.

https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case

<sup>&</sup>lt;sup>19</sup> J. Nathan Matias, Jonathan Penney, Merry Ember Mou and Max Klein (2020). "Do Law Enforcement Bots Reduce Freedom of Expression Online? Study Results". *EAT Lab.* 

<sup>&</sup>lt;sup>21</sup> ACLU (2021). Time and Again, Social Media Giants Get Content Moderation Wrong: Silencing Speech about Al-Aqsa Mosque is Just the Latest Example.

https://www.aclu.org/news/free-speech/time-and-again-social-media-giants-get-content-moderation-wrong -silencing-speech-about-al-agsa-mosque-is-just-the-latest-example/

<sup>&</sup>lt;sup>22</sup> Malachy Browne (2017). "Youtube removes Videos showing Atrocities in Syria." *The New York Times* August 22 2017.

<sup>&</sup>lt;sup>23</sup> Betsy Swan (2017) "Exclusive: Facebook Silences Rohingya Reports of Ethnic Cleansing" *Daily Beast* September 18 2017.

https://www.thedailybeast.com/exclusive-rohingya-activists-say-facebook-silences-them

<sup>&</sup>lt;sup>24</sup> Cat Zakrzewski (2020). "The Technology 202: Instagram faces backlash for removing posts supporting Soleimani." The Washington Post January 13 2020.

https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2020/01/13/the-technology -202-instagram-faces-backlash-for-removing-posts-praising-soleimani/5e1b7f1788e0fa2262dcbc72/



could lead to further suggestions on how to shorten the window without snaring overwhelmingly lawful speech in the process.

Recommendation: No mandatory time window should be put on content takedown decisions by platforms on individual pieces of content.

ii) Content moderation will never be completely unbiased

Content moderation decision-making will always be subjective, and cannot always be distilled down to a clear yes or no answer. Yet the consultation's proposal would require that automated decision making it mandates platforms adopt would not result in "any differential treatment of any group based on a prohibited ground of discrimination;" a requirement that is simply not possible – for online platforms, or for anyone.<sup>25</sup>

Both automated and human moderation have been shown to be rife with errors that are biased against members of protected groups.<sup>26</sup> Moderators, and moderation systems are well-known for making frequent mistakes. Combining algorithmic and human judgement does not undo these errors: it is more likely to conceal and reinforce them.<sup>27</sup>

While there's no 'right', unbiased way to do content moderation, there are many bad ways to do it. The inflexibility and punitive one-sided consequences of the government's proposal guarantees that online platforms will make their existing content moderation systems even worse.

At present, major corrections in content moderation processes on major platforms most often occur following independent journalism or internal leaks.<sup>28</sup> The independent, non-governmental source of these revelations and improvements is welcome and appropriate for monitoring globally relevant online platforms; their piecemeal nature is not.

Recommendation: Mandate independent, non-governmental and public auditing and transparency around content moderation tools and algorithms.

iii) Proactive surveillance obligations are unfit for democratic use

https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3921216

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC, Canada V5L 5G3 // 1-888-441-2640

<sup>&</sup>lt;sup>25</sup> Department of Canadian Heritage (2021). Technical Paper Para. 10a.

https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html <sup>26</sup> Maarten Sap, Dallas Card, Saadia Gabriel, Yeiin Choi, and Noah A Smith (2019), "The Risk of Racial

Bias in Hate Speech Detection" Association for Computational Linguistics (2019:1668-1678). https://aclanthology.org/P19-1163.pdf

<sup>&</sup>lt;sup>27</sup> Ben Green (2021). "The Flaws of Policies Requiring Human Oversight of Government Algorithms". SSRN

<sup>&</sup>lt;sup>28</sup> Jeff Horwitz (2021). "Facebook Says its Rules Apply to All. Company Documents Reveal a Secret Elite That's Exempt." *Wall Street Journal* September 13, 2021.

Paragraph 10 of the consultation paper requires platforms to proactively surveil user posts for the five forms of illegal content treated by this proposal, using automated tools. This is an astonishingly overreaching and disproportionate measure that has been roundly criticized and rejected in other jurisdictions, even in much more narrowly scoped form.

Algorithmic detection is the only way to fulfill a proactive detection obligation at any meaningful scale. Yet algorithmic detection is extraordinarily prone to errors in detecting illegal material, particularly for heavily context-dependent speech such as hate speech, incitement to violence and terrorism. Major platforms currently use it judiciously for only the most easily detectable material, such as child sexual exploitation material, precisely because it is so error-prone for more general purposes.

Forcing more generalized adoption of automatic detection of illegal content will sharply increase the misidentification and removal of lawful content, particularly of socially sensitive and political speech. For this reason, multiple UN Special Rapporteurs, the Council of Europe, and the global Manila Principles have all warned against states adopting a proactive content detection or filtering obligation.<sup>29 30 31</sup>

Recommendation: Do not mandate proactive surveillance by platforms, especially of more context-dependent harms.

iv) Direct reporting to law enforcement treats all Internet users as criminals

The consultation's technical paper proposes that user posts and account information should be automatically and secretly turned over to law enforcement when platforms remove a post as potentially constituting one of the targeted five forms of illegal content. This is one of the most egregious aspects of the proposal, and is an astonishing data and power grab for law enforcement. This process directly circumvents the critical checks and balances we have in place to prevent abuse of power, over policing and surveillance of millions of innocent people in Canada.

In effect, it would create a mass surveillance system of much lawful speech by Canadians and non-citizens alike who have committed no crime. It must absolutely **not** be in any proposed legislation.

https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gld=24234

<sup>30</sup> Council of Europe (2018). Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of Internet intermediaries.

https://rm.coe.int/1680790e14intermediaries

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC, Canada V5L 5G3 // 1-888-441-2640

9

medi

<sup>&</sup>lt;sup>29</sup> Joseph Cannataci, UN Special Rapporteur on the right to privacy; David Kaye, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; Fionnuala Ní Aoláin, UN Special Rapporteur on the promotion and protection of human rights and fundamental freddoms while countering terrorism. Open letter from Dec 2018:

<sup>&</sup>lt;sup>31</sup> Manila Principles on Intermediary Liability (2015), https://www.manilaprinciples.org/



The unbalanced platform incentives described earlier in this response will mean that the majority of removed content under the consultation's system will not actually constitute illegal content. It will consist of normal user activity that platforms remove because they can, and because any legal risk to them, even at a relatively low probability, is more important than silencing their user base.

By virtue of all flagged content being directly reported to law enforcement, countless Internet users will exist in databases alongside criminal content, in many cases simply because someone else on the platform flagged their content – often simply because they dislike it. Worse yet, the proposal fails to contain a single adequate indication that there would be any accountability for how law enforcement manages, retains, or deletes the data (if it ever does).

This type of law enforcement lawful access to user data has already been proposed, and rejected, numerous times in the past – perhaps most infamously in the debate surrounding 2011's *Bill C-30, The Protecting Children from Internet Predators Act.*<sup>32 33</sup> The government must not support or create a surveillance state, proactively monitoring innocent internet users.

It is worth noting that Law enforcement in Canada is already flooded with many times more reports of hate crimes than they have the resources or willingness to act on.<sup>34</sup> Even complaints filed directly by those who feel a crime has been committed against them, are often ignored. Automatic reporting of online takedowns will make this situation many times worse, with agencies deluged with an ocean of online reports from platforms, the great majority of no real use.

OpenMedia is concerned this ocean of mostly lawful speech would serve only one meaningful purpose: the extra-judicial creation of an immense trawling net for law enforcement to target and gather intelligence about individuals who have committed no crime, but nonetheless attract attention from police and the powerful, including Indigenous activists, environmental movements, and members of otherwise marginalized ethnic and religious communities.

It is also worth emphasizing that platforms hold an almost unimaginably rich volume of information about their users, including their website traffic, likes and dislikes, commuting routes and geographic locations, detailed social networks, inferred current emotional states, and more. This is not only dangerous in the hands of a single company – an issue the government seems unwilling to address in its abandonment of its own privacy legislation in the last session of

<sup>32</sup> Government of Canada (2012). "An Act to enact the Investigating and Prventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts" https://www.parl.ca/LEGISInfo/BillDetails.aspx?Language=E&billId=5375610

<sup>33</sup> OpenMedia (2012). A look back at our Stop Spying campaign against Canada's Bill C-30 https://openmedia.org/look-back-our-stop-spying-campaign-against-canadas-bill-c-30

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC, Canada V5L 5G3 // 1-888-441-2640

<sup>&</sup>lt;sup>34</sup> Mike Hager, "Alleged hate crimes rarely investigated by police, report claims," *Globe and Mail*, August 30 2021.

https://www.theglobeandmail.com/canada/british-columbia/article-alleged-hate-crimes-rarely-investigatedby-police-report-claims/



parliament – but is wildly inappropriate information for law enforcement to have about innocent internet users, without needing to demonstrate a clear need and threat, and obtain a warrant.

Until our government restricts the vast data platforms collect on us, a requirement for platforms to turn over user data in any circumstances outside clear and imminent threat to life or a confirmed serious crime presents an enormous threat to the right to privacy of people in Canada.

Canada is a democratic country, which cannot and must not treat all of its citizens as criminals. This proposal directly undermines the criminal justice system, our legal checks and balances on abuse of power, and puts Canada on par with some of the world's most oppressive governments.

Recommendation: Do not require reporting of user posts or information by platforms to law enforcement for anything less than clear and immediate threat to life, or once content has been deemed explicitly illegal. Do not mandate ANY automatic reporting to law enforcement.

v) Website blocking is disproportionate, ineffective, and unwelcome in Canada

The consultation paper proposes exceptional recourse that would require ISPs to block access to platforms if the platform repeatedly fails to remove child sexual exploitation material or terrorist content, and other enforcement mechanisms have been exhausted.<sup>35</sup>

It is assumed that this proposal is not targeted at mainstream online platforms, who generally already make adequate efforts to remove both these types of content. Even for smaller platforms, however, website blocking is deeply ineffective at its stated purpose, being easy to circumvent, and therefore very unlikely to deter highly motivated individuals seeking the abhorrent content described. Technologies such as VPNs, proxies servers, and Tor browser are widely available, and must remain so to allow millions of Internet citizens who live under oppressive regimes to communicate and access information, as their Internet is otherwise highly controlled and censored.<sup>36</sup>

The chief consequence of a website blocking regime would be removing access to mixed use platforms from their users who have no connection to illegal content, and are using the platforms legitimately.

As the Department is well aware, website blocking is not a new or uncontroversial issue in Canada. Despite widespread public opposition, the tactic has been proposed for Canada year

<sup>35</sup> Department of Canadian Heritage (2021). Technical Paper Para. 120.

https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html <sup>36</sup> Electronic Frontier Foundation (2020). Understanding and Circumventing Network Censorship https://ssd.eff.org/en/module/understanding-and-circumventing-network-censorship

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC, Canada V5L 5G3 // 1-888-441-2640



after year by media conglomerates who would like to make it harder for Canadians to access media from other countries without paying them for content that they've licensed.

It has been also been rejected by the CRTC and Parliament repeatedly as neither a proportionate nor effective remedy<sup>37 38</sup>. Yet this year the government again proposed the remedy, in its Consultation on a Modern Copyright Framework for Online Intermediaries and was, again, met with widespread opposition concerned with the inappropriate and ineffective government overreach. OpenMedia expressed our concerns with this proposal in more detail earlier this year during this consultation.<sup>39 40</sup>

Recommendation: Effective website blocking for highly motivated individuals is not technically feasible. The government should abandon its consideration for these purposes, and focus on developing our relationship with other jurisdictions to address services that intentionally host child sexual abuse material or terrorist content.

#### vi) Legal remedies must use the court system

Some portions of the government's proposal appear to be efforts to 'simplify' the process of assessing the legality of user posts by circumventing our existing legal process. Not only will this simplification not work, it will directly undermine and overload our existing legal system.

The Digital Recourse Council described in the technical paper consists of an appointed group of 3-5 people, with sensitivity to representation from Canada's diverse populations, but without an expressed requirement for legal or constitutional expertise or counsel.

It seems improbable that this small group will have the capacity or expertise required to deal with the volume of claims they will receive under this system. Countless groups and individuals will have a legitimate interest in having their right to express themselves reinstated by the Council, or illegality of others' content confirmed. The volume of cases brought before a body this small could lead to queues of many years for clear consolidation and response.

Whether the Council can manage the volume of appeal or not, it is unclear what value it is adding to the existing system. If its role is strictly to resolve relatively unambiguous applications

https://www.ic.gc.ca/eic/site/693.nsf/eng/00191.html

<sup>40</sup> OpenMedia (2021). OpenMedia Submission to the Copyright Consultation on a Modern Framework for Online Intermediaries.

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC, Canada V5L 5G3 // 1-888-441-2640

<sup>&</sup>lt;sup>37</sup> OpenMedia (2021). Thousands of OpenMedia community members just stood up to defend Canada's Internet from website blocking!

https://openmedia.org/article/item/thousands-openmedia-community-members-stood-up-defend-canada-internet-from-website-blocking

<sup>&</sup>lt;sup>38</sup> OpenMedia (2018). Huge win for Canadians as CRTC rejects Bell's website blocking proposal, https://openmedia.org/press/item/huge-win-canadians-crtc-rejects-bells-website-blocking-proposal-title\_d uplicated

<sup>&</sup>lt;sup>39</sup>Innovation, Science, Economic Development Canada (2021). *Consultation on a Modern Copyright Framework for Online Intermediaries.* 

https://openmedia.org/files/OpenMedia - Submission to Online Intermediary Consultation.pdf

of Canadian law, it is not clear why the Council itself is necessary. If it is intended to issue interpretative judgements, changing or reducing the current understanding of freedom of expression rights on online platforms compared to offline spaces, it would appear to be plainly usurping the rightful and necessary role of our court system.

If that usurpation is recognized and the Council is regularly overruled by our courts, the system will have been a waste of time and money, particularly for the victims and defendants forced to use it. If that usurpation is not recognized, we will have an extra-judicial system setting legal precedents in our country, which would be even more concerning.

# Recommendation: Extra-judicial bodies cannot be put in the position of setting legal precedent. If legal clarification is required of how to apply Canada's laws on platforms, that must be a judicial responsibility.

vii) An all-powerful regulator is not the answer

A key mistake in this consultation is attempting to address too many disparate issues on the Internet with the same regulatory agent and power. Direct threats to human life, threats to property, the non-consensual distribution of sexual imagery, sexually exploitative material involving children and hate speech are very different issues. They differ in the immediacy and severity of potential harm, appropriate rights to information, appeal, and decision-making for victims and accused persons, and necessary legal and contextual expertise for a hypothetical regulatory body or agent.

By attempting to handle all of these harms through a single body and piece of legislation, the government is creating equally invasive powers, detection standards, and potential penalties in each case. This creates a slippery slope in which powers that could be justified for the most extreme potential harm are available to the regulator for very different smaller or contested cases. It is likely to lead to disproportionate procedures used in many cases not justified by their actual harm. This is even more likely given that a single overstretched regulator will lack the capacity to wisely and contextually interpret the full range of cases brought before it.

It also leaves on the table the potential for much more nuanced issue-sensitive remedies tailored to the type of violation. For example, independently managed hashed image databases have proven effective as a non-legislative tool for reducing the spread of child sexual exploitation material on online platforms. They may also have value as a solution for removing non-consensually distributed adult intimate imagery (NCDII), given that the impacted adults could verify their ID to the body and request its removal. Yet hashed databases would not be appropriate for removing evidence of promotion of terrorism or hate speech, since this content is more ambiguous in status and meaning, and society has many valid purposes for accessing it, including journalism, research, and documentation of real-world abuse.<sup>41</sup>

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC. Canada V5L 5G3 // 1-888-441-2640

13

media

<sup>&</sup>lt;sup>41</sup> Danielle Citron and Neil M. Richards (2018). "Four Principles for Digital Expression (You Won't Believe #3!)", *Washington University Law Review* (Vol 95:1353-1387:2018). https://wustllawreview.org/wp-content/uploads/1353-1387-Citron-Richards\_Final.pdf



The astonishing breadth of power assigned to the proposed Digital Safety Commissioner, including the power to compel online platforms "to do any act or thing, or refrain from doing anything," seems a sign of a real lack of clarity about what the creation of the Commissioner's position is actually trying to accomplish.<sup>42</sup> This is not an appropriate approach to creating an extremely powerful new body in a democratic society, particularly one governing an area as sensitive as online speech.

Recommendation: Do not to address all five forms of illegal content through the same system and procedures. Consult with scholars and issue experts about appropriate solutions to each. At a future consultation, publicly discuss all the options suggested and solicit opinions on them.

Recommendation: Any powers granted to a new or existing regulator over online platforms and online speech must be carefully defined, explained, justified, and clearly limited.

#### viii) The proposal will harm those it claims to help

This proposal is presented as a strategy to combat online hate, and better protect marginalized communities online. That makes it worth reviewing the ways it will significantly harm and worsen the experience of many marginalized people and victims of online attacks.

- 1) Censoring the speech of marginalized communities: It is clear to see how marginalized communities are already targeted online with hate, harassment, and abusive behaviours. Yet their ability to discuss this victimization, share examples of hate speech directed at them, and push back against that speech will be badly damaged by the predictable consequences of the consultation's proposals. Due to the clear incentives the proposal gives platforms to aggressively remove speech without much sensitivity to context, platforms will insensitively remove far more speech from targeted groups around their experience of social marginalization, and descriptions of the attacks others make on them. This is not hypothetical platform behaviour; it is already a common issue, without these new legal incentives that will strongly reinforce it.<sup>43</sup>
- 2) Enabling online hate: Counter-intuitively, forcing rigid content moderation rules on platforms will super-charge troll brigades who already use platform rules to attack marginalized individuals. No one knows the exact limits of a given platform's rules for

<sup>42</sup> Department of Canadian Heritage (2021). *Technical Paper* Para. 80.

https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html <sup>43</sup> Jessica Guynn (2019). "Facebook while black: Users call it getting 'Zucked,' say talking about racism is censored as hate speech." USA Today April 24, 2019.

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC, Canada V5L 5G3 // 1-888-441-2640

https://www.usatoday.com/story/news/2019/04/24/facebook-while-black-zucked-users-say-they-get-block ed-racism-discussion/2859593002/

OpenMedia is a community-based organization that safeguards the possibilities of the open Internet.



a su merana a Inhonwhan

speech like some members of hateful online communities do, and no one is better at communicating hateful views while staying within those rules, while studiously observing their targets for pushback or past posts that might violate them.<sup>44</sup> The only way for platforms not to fall prey to this kind of rules lawyership is to continue giving platforms space to exercise judgment and flexibility in applying their own rules.

3) Enabling law enforcement surveillance and over-policing of marginalized communities: It is difficult to imagine a more powerful engine of over-policing of marginalized communities than giving law enforcement who already operate with bias an overwhelming volume of content takedown reports, and letting them pick and choose which to try to criminally enforce. Law enforcement surveillance of lawful marginalized communities is already a problem in Canada; the provisions described in the consultation will make it a much, much larger one.<sup>45</sup>

#### ix) Setting a dangerous precedent with global ramifications

Content posted to the Internet does not exist within a single national jurisdiction. Posts are available globally, and there is no easy way for platforms to justify that some national laws should apply to a given piece of content, but not others.

It is a deeply unreasonable expectation of this consultation's proposals that platforms will separately consider the nuance of law around expression within each jurisdiction they function in, for each piece of content, and individually mark content to be removed in only some jurisdictions.

As with other legal patchworks, a much more likely longer-term outcome is that platforms will take the broadest interpretation of Canada's laws on content takedowns, and combine it with broad interpretation of similar law in other jurisdictions, to create a single global standard for their moderation that universally protects them from legal threat.

This amalgamated standard would be systematically biased against freedom of online speech. The product would not be a product of the thoughtful weighing of the expressive rights of users versus removing illegal content that exists in any given democratic legal system, but rather a kind of race to the bottom for restrictions on user speech. Any overly broad law in any jurisdiction that poses a credible legal or financial threat to platforms would have the potential to become universalized, and limit expression across the global Internet.

https://institute.global/policy/social-media-futures-what-brigading

<sup>45</sup> Bruce Livesey (2017). "Spies in our midst: RCMP and CSIS snoop on green activists". *National Observer* May 5 2017.

https://www.nationalobserver.com/2017/05/05/news/spies-our-midsl-rcmp-and-csis-snoop-green-activists

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC. Canada V5L 5G3 // 1-888-441-2640

<sup>&</sup>lt;sup>44</sup> Phoenix CS Andrews (2021). "Social Media Futures: What is Brigading?" *Tony Blair Institute for Global Change*.

There's one alternative, and it is even worse: Canada doing its part to usher in the so-called 'Splinternet'.<sup>46</sup> In a Splinternet model, large parts of the Internet are fenced off by restrictive national legislation controlling what comes in or out. This is not only what Canada is proposing, but an incredibly dangerous precedent for Canada to encourage, in terms of what it means for regulation by other governments of online content. Currently, major platforms are amongst the primary bulwarks against the emergence of splinternets, as their independent content standards make restrictive national censorship by governments more difficult. If Canada is successful in forcing many platforms to tailor their content systems to a specific government model, but only for Canadian users or within Canadian IP addresses, we will not only be building a shallow Splinternet of our own. But we'll also be furthering the legitimacy of much more restrictive Splinternets elsewhere.

This is only furthered by the proposals to directly tie these content regulations to law enforcement reporting requirements, something that could lead to the direct persecution of millions of Internet users globally who currently use online platforms as one of the few areas they are able to express themselves.

## C. What a better discussion of online harms might look like

I) Clearly separate illegal content from online harms

The government's continued pattern of conflating discussions of illegal content and other problems with legal speech online is deeply concerning. Throughout this proposal, the distinction is blurred, with the term 'harmful content' used as a stand-in for illegal content.

Outside of this proposal, Minister Guilbeault has spoken of problems of online civility, misinformation, and rude language directed at politicians as types of harmful online content that the government is concerned with addressing.

It is not, and can never be the government's role to police online civility or factualness. That's not a power that is safe for any government to have, or that people in Canada will tolerate.

The power to criminalize and remove speech from the Internet, either directly or functionally by foreseeable consequences of your legislation, must be handled extraordinarily carefully. Any new regulation must be restricted to illegal speech, with careful attention to whether it is disproportionately leading to removal of legal speech, as we've argued above.

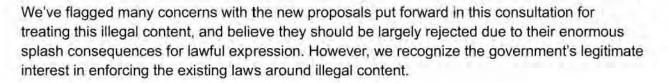
Moving forward from this consultation, it is critical that the government be extremely clear about when it is speaking about illegal content, plainly falling within the five forms of illegal content described in the consultation paper, and when it is speaking of other issues on the Internet.

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC, Canada V5L 5G3 // 1-888-441-2640

16

media

<sup>&</sup>lt;sup>46</sup> Jeff John Roberts (2019). "The Splinternet is Growing" Fortune May 29, 2019. https://fortune.com/2019/05/29/splinternet-online-censorship/



Toxic and harmful behaviour clearly exists on the Internet outside these forms of illegal content. But the government's appropriate role in contributing to addressing these issues is not the blunt enforcement of mass content removal, without context or accountability.

#### ii) Addressing the knowledge gap around harmful online content

Calls for further research can be read as a call to do nothing. But content moderation at the scale online platforms deal with has existed for barely 10 years, and is still very poorly understood. As content moderation scholar Evelyn Douek writes, it is "striking how much we do not know about online speech... we are only at the very beginning of the process of determining what works, outside of the take-down/leave-up paradigm."<sup>47</sup>

Further research isn't just necessary: it is the single most important thing we need to do. No sound policy can be designed without much more information on how people actually respond to different levels and types of content moderation.

There are two enormous gaps in our understanding of both illegal content, and lawful but harmful content and behaviour online – and our government could very productively contribute to both.

The first is a data gap; despite years of pressure, platforms resist requests for them to share data they hold on how their platforms are impacting their users. Data is provided to researchers looking to understand content moderation grudgingly, often incomplete, and withdrawn at the slightest sign of controversy or bad press.<sup>48</sup> Platform users are given obscure, misleading or incomplete accounts of what data platforms hold on them, and how or why their content has been promoted or moderated. As a result, we rely far too much on occasional leaks from platform whistleblowers to understand how platforms are affecting us, both collectively and individually.

Documenting the impact of social media spaces and algorithms on us is much too important to be restricted to internal platform reports, as platforms have a vested interest in burying or minimizing findings that are bad for business. As such, OpenMedia endorses legislating detailed transparency requirements for all major online platforms on how they're moderating content,

<sup>48</sup> Taylor Hatmaker (2021). "Facebook cuts off NYU researcher access, prompting rebuke from lawmakers" *Techcrunch* August 4 2021. <u>https://techcrunch.com/2021/08/04/facebook-ad-observatory-nvu-researchers/</u>

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC. Canada V5L 5G3 // 1-888-441-2640

<sup>&</sup>lt;sup>47</sup> Evelyn Douek (2021). "Governing Online Speech: From "Posts-as-Trumps" to Proportionality and Probability" *Columbia Law Review* Vol 121 No.3 page 819 (April 2021)



CLED IN TRIBLE & FORMULAR

including how much and what type of content is removed, appended with fact-checking labels, or consciously downranked.

We recognize some language supporting increased transparency in the consultation paper, but it cannot be provided just to a closed Canadian regulator.<sup>49</sup> Detailed transparency reports must be made available to all users of a platform, and the opportunity to study data and audit algorithms made available to qualified academic researchers, not only government.<sup>50</sup> As Douek writes, the goal should be "to expose to public scrutiny the decision-making process already taking place, so that it can be subject to public argumentation, contestation, and disruption."<sup>51</sup>

The data gap has fed a research gap on questions that are essential to making good decisions moving forward on how to support user expression online while limiting damaging outcomes. There is an overwhelming need for more research on how users are interacting with each other in legal but negative ways, including having negative or toxic interactions, spreading misinformation, and making use of or being failed by content takedown mechanisms. Innovative ideas for approaches that could better balance user expression with mitigating potential harms abound, including making it easier for users to block or hide certain types of posts, warning labels, small nudges to read articles before sharing, or demonetizing certain types of content around important and sensational issues.<sup>52 53</sup>

We are not recommending any of these approaches; more research is needed to determine whether they're effective to their purpose, and what their side consequences could be. We're pointing to them as examples of areas where more research could reveal rights-protective solutions to some online problems.

Support for research on content moderation and partnerships with platforms is referred to in a single vague mention in the consultation's technical paper.<sup>54</sup> Yet this is a key area that the government could make a meaningful difference to with further attention and support.

## Recommendation: Mandate detailed, open and public transparent reporting on how content moderation practices are applied to online platforms.

https://ijoc.org/index.php/ijoc/article/view/9736/2610

<sup>52</sup> Evelyn Douek (2021). "Governing Online Speech: From "Posts-as-Trumps" to Proportionality and Probability" *Columbia Law Review* Vol 121 No.3 page 826 (April 2021)

<sup>53</sup> Ben Kaiser, Jonathan Mayer, J. Nathan Matias (2021). "Warnings that Work: Combating Misinformation Without Deplatforming." *Lawfare Blog.* 

https://www.lawfareblog.com/warnings-work-combating-misinformation-without-deplatforming. <sup>54</sup> Department of Canadian Heritage (2021). *Technical Paper* Para. 35b.

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC, Canada V5L 5G3 // 1-888-441-2640

<sup>&</sup>lt;sup>49</sup> Department of Canadian Heritage (2021). *Technical Paper Para*, 14.

https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html <sup>50</sup> Nicolas Suzor, Sarah West, and Jillian York. "What Do We Mean When We Talk About Transparency? Toward Meaningful Transparency in Commercial Content Moderation" *International Journal of Communication 13(1526-1543)*.

<sup>&</sup>lt;sup>51</sup> Evelyn Douek (2021). "Governing Online Speech: From "Posts-as-Trumps" to Proportionality and Probability" *Columbia Law Review* Vol 121 No.3 page 819-820 (April 2021)

https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html



Recommendation: Explore legal requirements to mandate online platforms share content moderation and user engagement data with independent research teams. Ensure any requirements show due consideration for platform user privacy.

Recommendation: Canada should be a global leader in funding research that seeks to better understand the patterns and drivers of both illegal content, and legal but potentially harmful user behaviour and content online.

#### iii) Empowering internet users; not Blg Tech

As Sue Gardner rightly points out, the government's current 'attack' on Big Tech targets symptoms of problems with the modern Internet, not the cause.<sup>55</sup> Most Internet users feel they have very little control over what they see, control, and are able to protect themselves from online.

This is facilitated by a world in which Internet users are data products for online platforms, not communities they are meaningfully accountable to. Online platforms largely make a living buying and selling access to our data, while keeping us on their platform for as long as they can. Illegal content is rarely welcomed by mainstream platforms, but emotionally upsetting and polarizing content that drives high user interaction can be harder for them to turn down. Many Internet users are frustrated by knowing they are being played by algorithms in this way, yet recognize they have little meaningful power to change their online experience.

The government seems to have succumbed to the tempting but deeply misguided approach of stepping in and attempting to assume the role of arbiter of what's good and bad on the Internet. It won't work for many reasons, including that many world governments are currently grappling with the same temptation, and they disagree on what ought to be considered good and bad. But as we've documented in this response, a failed attempt to exercise that enormous governing power could do a great deal of damage to people's speech and experience online before playing itself out.

Smart government regulation should focus on empowering Internet users to retake control of their own respective online experiences, and effectively pressure Big Tech platforms.

First, it needs to be made much easier for Internet users to leave a platform, taking all their personal data with them, without severing their ties with friends and family left on the platform. This means bringing back a version of the last parliament's *Bill C-11*, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act* 

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC, Canada V5L 5G3 // 1-888-441-2640

<sup>&</sup>lt;sup>55</sup> Sue Gardner (2021). "The crackdown on 'Big Tech' targets symptoms rather than the disease itself' *Globe and Mail* May 21, 2021.

https://www.theglobeandmail.com/opinion/article-the-crackdown-on-big-tech-targets-symptoms-rather-than-the-disease/



and to make related and consequential amendments to other Acts, and patching its many holes to make it strong and effective legislation, such that users have a strong and easily actionable right to access, modify, delete, and transfer their data held by any company.

It is striking that despite Bill C-11's introduction in November 2020, promising major reform of our privacy rights in the private sector, the government made no effort to actually pass the Bill, let alone fix the many loopholes and areas that needed tightening identified by privacy experts. We hope to see that change in our next Parliament.

If effective user control of our data was combined with strong transparency and research requirements, platforms would find themselves with a user base that can easily leave a platform they're dissatisfied with. This would allow users themselves to effectively pressure platforms to reform themselves if their content moderation or privacy standards are not adequate.

Second, a hard, data- and research-driven look needs to be taken at whether an advertising and 'time spent on platform' business model is compatible with the needs of healthy democratic discourse. This business model demands engagement above all else, and that includes a lot of deeply negative engagement. Without addressing the underlying business models and incentives, the problems the government aims to tackle here will remain fundamentally unsolved.

Throughout, the government must consider whether their approach is encouraging a reduction of major platform power, or reinforces and depending on it. A recurring theme in scholarly discussion of the power of Big Tech is the need to avoid regulatory 'lock-in' of their power and prominence.<sup>56 57</sup>

Expensive and complex regulatory obligations make it difficult for new online platforms to compete with the handful of platforms that dominate our Internet today. That's why they can be surprisingly popular with some of the largest entrenched platforms.<sup>58</sup>

But careful government legislation could erode that dominance. Some online platform dominance comes from making good products, but much of it comes from translating early leads in the market into runaway network effects. The more people use a given platform, the more valuable being on that platform becomes. Over time, online platforms have converted their platforms into so-called 'walled gardens' – trapping many users who do not necessarily approve of their practices or want to be on their service.

https://cacm.acm.org/magazines/2021/10/255710-competitive-compatibility/fulltext

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC, Canada V5L 5G3 // 1-888-441-2640

<sup>&</sup>lt;sup>56</sup> Cory Doctorow (2021). "Competitive Compatibility: Let's Fix the Internet, Not the Tech Giants" *Communications of the ACM*, Vol 64, No. 10 (October 2021).

<sup>&</sup>lt;sup>57</sup> Evelyn Douek (2021). "Governing Online Speech: From "Posts-as-Trumps" to Proportionality and Probability" *Columbia Law Review* Vol 121 No.3 page 829-830 (April 2021)

<sup>&</sup>lt;sup>58</sup> Amanda Macias (2020). "Facebook CEO Mark Zuckerberg calls for more regulation of online content" CNBC Feb 15 2020.

https://www.cnbc.com/2020/02/15/facebook-ceo-zuckerberg-calls-for-more-government-regulation-online-content.html

There are many innovative ideas currently being explored about how content moderation could be done better on a less Big Tech centered web. Recent proposals have included separating content moderation from platform responsibility as an independent form of 'middleware'; developing competitive content moderation protocols that individual users can adopt to provide the type of protection they want on the web; encouraging 'trusted flaggers' systems, in which users whose reports of illegal content are consistently valid have expedited processing time; and instituting a duty of care on platforms for their users, less focused on case by case outcomes and more systematically evaluative of how they approach their overall responsibility to user safety and wellbeing.<sup>59 60 61 62</sup>

We are not endorsing any of these approaches; more research is needed to evaluate their potential effects. But they should at least be considered in a more appropriately open and thoughtful future consultation from the government.

Recommendation: Empower Internet users against Big Tech. Give them the rights they need to leave platforms they don't like, and they can hold platforms accountable themselves to moderate content responsibly.

Recommendation: Many lawful but harmful online behaviour and user experiences are driven by an ad-centric business model that works to keep users on a platform at any cost. Solicit ideas for regulatory remedies that would discourage the proliferation of this model.

Recommendation: Ensure that any new regulation discourages the centralization and concentration of online platforms.

## D. Conclusion

This response is not wholly comprehensive of OpenMedia's concerns with the government's apparent intended direction for our Internet; it is only the beginning of that conversation.

We are a community that is immensely passionate about the tremendous liberating power of the open Internet. That does not make us enemies of all ideas for regulating it, as we trust we've made clear.

OpenMedia Engagement Network // 1424 Commercial Dr - P.O. Box 21674, Vancouver, BC, Canada V5L 5G3 // 1-888-441-2640

21

media

<sup>&</sup>lt;sup>59</sup> Francis Fukuyama (2021). "Making the Internet Safe for Democracy." *Journal of Democracy* Vol 32(2):37-44.

https://www.journalofdemocracy.org/articles/making-the-internet-safe-for-democracy/

<sup>&</sup>lt;sup>60</sup> Mike Masnick (2019). "Protocols, not Platforms: A Technological Approach to Free Speech." *Knight First Amendment Institute at Columbia University*.

https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech <sup>61</sup> Darryl Carmichael and Emily Laidlaw (2021). The Federal Government's proposal to Address Online Harms: Explanation and Critique

https://ablawg.ca/2021/09/13/the-federal-governments-proposal-to-address-online-harms-explanation-and -critique/

<sup>&</sup>lt;sup>62</sup> Daphne Keller (2020). "Systemic Duties of Care and Intermediary Liability." Blog entry: http://cyberlaw.stanford.edu/blog/2020/05/systemic-duties-care-and-intermediary-liability



We whole-heartedly reject the very nature of this consultation and manner in which it has been held, in addition to the specific proposals currently being proposed. As we've laid out, this proposal will overwhelmingly censor lawful speech more than illegal content, produce an unprecedented surveillance funnel of lawful speech to law enforcement, and hurt marginalized communities far more than it will help them.

But we've also highlighted many measures our government could take now that would genuinely take on and roll back the power of major online platforms, while contributing to a healthier and less hateful Internet. These include strong data ownership, research and transparency reporting changes that would make platforms far more accountable to their users, and highlighting some interesting ideas for more innovative content moderation models that would make a more genuine future public consultation on these issues far more fruitful.

We'll close with a fundamental question; what do Canadian Internet users actually want for our Internet? How would they like to see their rights defended, and their content moderated?

It is unclear that our government wants to find out, preferring to use single answers to generic poll questions to justify their current intentions. That needs to change.

Due to the nature of this consultation, and the short timeline, this submission only represents a fraction of our community's concerns and perspectives. But we hope they have helped to highlight just how damaging this current proposal is to not only the internet in Canada, but globally.

We represent some of the most concerned and engaged people in Canada on these issues, and will continue to make ourselves heard by our elected officials and representatives, whether the government provides appropriate formal opportunities to do so, or not.

Matthew Marinett

Comments on the Government's proposed approach to address harmful content online

September 25, 2021

## Comments on the Government's proposed approach to address harmful content online

Thank you for the opportunity to provide feedback on this proposal. As a doctoral candidate at the University of Toronto Faculty of Law studying internet regulation, I am happy that the current government takes the issue seriously and has begun considering regulatory approaches to address harmful content on the internet. Regulating online harms is an important goal and one that can benefit from a uniquely Canadian approach, not unlike our innovative approach to copyright online.

Unfortunately, a uniquely Canadian approach is not what has been presently proposed by the Government of Canada. Instead, the current proposal appears to cobble together various proposals or regimes seen in other jurisdictions without meaningfully considering either their likelihood of success or their impact upon freedom of expression and privacy in the Canadian context. The result is that the proposed legislation would negatively impact the human rights of Canadians while failing to achieve the core aims of the proposals.

In my view, there is little in the current proposal to commend, and I would recommend that the Government revisit the issue through robust consultations with academics, eivil society and stakeholders to craft a viable regulatory regime with a real capacity to limit online harms and ensure democratic control of our online information ecosystem.

Others, such as Darryl Carmichael and Emily Laidlaw <u>have laid out the core problems</u> with the current proposal, and I agree with many of their critiques and recommendations. My comments here focus on explaining how the current proposals are likely to interact with platforms and users to demonstrate how the proposals will fail to achieve their desired ends while raising a number of important concerns.

My comments focus on four issues: to whom the proposed legislation applies, general monitoring obligations, twenty-four-hour timelines to address flagged content, and mandatory reporting to law enforcement. I conclude with some overarching observations and recommendations.

## Scope of the Regulation

## The proposed legislation risks being over-inclusive or under-inclusive

The Technical Paper does not make it clear what the definition of an Online Communication Service Provider (OCSP) would be. The Discussion Guide indicates that it would capture "major platforms" such as Facebook, TikTok, Twitter etc., while not applying to, for example, travel review sites (presumably such as Tripadvisor). It's not currently clear on what basis this distinction is to be made.

Encounted constants for service la Leo anti-catale e Pollonischer Die meent released recording for Die Access recording method

#### Matthew Marinett

Comments on the Government's proposed approach to address harmful content online

Regardless of the criteria for inclusion in the definition of an OCSP, the approach currently taken appears to be one in which the legislation either applies to an internet intermediary or it does not. While I note that paragraph 17 of the discussion paper contemplates the Digital Safety Commissioner making regulations that tailor requirements to different categories of OCSPs based on the "distinct business models, sizes, and resources of various OCSPs," it's hard to see what obligations would be so tailored, or how. Regardless, the definition of OCSP will apparently exclude a significant set of internet intermediaries, and those that are included would face significant requirements, including responding to flagged content within twenty-four hours, taking reasonable measures to monitor content, and reporting to law enforcement. This is in contrast to the European Union's proposed *Digital Services Act* (DSA), which captures many intermediaries, but expressly provides for a tiered structure in which internet intermediaries are subject to increasing obligations in accordance with the kind of service they provide and their user base.

The approach contemplated in Canada's proposal risks either being over-inclusive or underinclusive, or both. If the definition is too wide, it will capture services that have no capacity to comply with the requirements and may destroy new market entrants before they can grow. This would only benefit the powerful incumbent services like Facebook that can more easily comply. If the definition is too narrow, however, it will do little to limit harmful content on the internet, as it will apply to only a handful of companies. While there is merit to limiting harmful content on the largest platforms, an under-inclusive definition will permit bad actors to easily continue to disseminate harmful content on other significant platforms. A better solution is to capture internet intermediaries broadly with carefully tailored and scaled requirements, such as in the EU's proposed DSA.

#### The legislation risks undermining innovative content moderation strategies

Not all major platforms rely on large numbers of paid content moderators to remove harmful content. Some, instead, rely on volunteer moderators and community leaders. It is notable that the Discussion Paper list Facebook, Twitter, YouTube, Instagram, and TikTok, and Pornhub as entities that would fall within the definition of an OCSP, but does not mention Reddit, which has a user base roughly equivalent to that of Twitter, or other similar sites. All of the sites listed in the Discussion Paper fall within what <u>Robyn Caplan has identified</u> as employing "industrial" content moderation, in which content is moderated primarily in a top-down manner by agents of the platform.

By contrast, Reddit uses "community-reliant" moderation, in which members of the user base itself engages in content moderation within Reddit's individual communities. While agents of Reddit do engage in some content moderation, the <u>significant majority</u> of content moderation actions are undertaken by Reddit users, including under Reddit's site-wide content policy. Should the definition of an OCSP capture Reddit, or other sites that use community content moderation strategies like Wikipedia, it's unclear whether the site would currently be able to comply with the requirements, given the need for centralized moderation to address flagged content within twenty-four hours. The legislation could thus have the effect of mandating certain content moderation strategies that demand hiring additional content reviewers. If platforms are

#### Matthew Marinett

Comments on the Government's proposed approach to address harmful content online

required to hire teams of dedicated content reviewers, this will undermine the impetus to develop innovative approaches to content moderation that could prove more effective than the kinds of industrial moderation contemplated by the proposal.

#### **General Monitoring Obligations**

The Technical Paper states that the act will provide that an "OCSP must take all reasonable measures, which can include the use of automated systems, to identify harmful content that is communicated on its OCS and that is accessible to persons in Canada, and to make that harmful content inaccessible to persons in Canada." The implication is that the legislation would require active screening, including through the use of automated systems, to detect designated content and render it inaccessible to Canadians. This is deeply problematic, as such detection systems are likely to negatively impact legitimate speech, especially that of vulnerable communities.

Harmful content, especially hate content and incitements to violence, is notoriously difficult to detect automatically and often requires an assessment of the context in which the content was communicated. It is difficult, for example, for an automated system to tell whether a photograph of a Nazi swastika is being posted in support of Nazism or whether it is being used to criticise or satirize government policies or oppose fascism. In other cases, legitimate educational posts may recreate historical content that clearly incites violence or promotes hatred; understanding the surrounding educational context will be difficult for many automated systems.

Most major platforms already use various automated monitoring systems to address terrorist content and child sexual abuse material using existing hash databases, such as PhotoDNA or via the Global Internet Forum to Counter Terrorism (GIFCT). And many already use algorithmic processes to address various additional kinds of harmful content, such as hate speech, where possible. However, while such systems may be employed by social media networks of their own accord, imposing significant potential sanctions for failures to use such systems risks chilling a great deal of legitimate expression by incentivizing aggressive over-blocking. As the <u>former UN</u> <u>Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression wrote about general monitoring requirements:</u>

such rules involve risks to freedom of expression, putting significant pressure on companies such that they may remove lawful content in a broad effort to avoid liability. They also involve the delegation of regulatory functions to private actors that lack basic tools of accountability. Demands for quick, automatic removals risk new forms of prior restraint that already threaten creative endeavours in the context of copyright. Complex questions of fact and law should generally be adjudicated by public institutions, not private actors whose current processes may be inconsistent with due process standards and whose motives are principally economic.

In other words, governments should not mandate that social media companies make rapid decisions about whether or not content meets legal definitions and take action on it, especially through automated systems and pre-publication blocking.

Comments on the Government's proposed approach to address harmful content online

Indeed, given that most major social media platforms already engage in some degree of ongoing monitoring of many kinds of harmful content, it's hard to see the benefit of this requirement for the kinds of entities falling within the definition of an OCSP. Either their current practices will remain unchanged, or their practices will become more aggressive, attempting to tackle the mode context-demanding cases which will certainly come at the expense of expression and legitimate speech. Existing content moderation practices already <u>disadvantage vulnerable communities</u>, and increasing the aggressiveness of content policing, like all aggressive policing, will prove disproportionately harmful to such communities. Anemic statements that the proposed Act will require OCSPs to ensure that such disparate treatment does not arise are of little value given it is unclear how such requirements could be meaningfully implemented or enforced.

For these reasons, any requirement mandating proactive general monitoring should not be considered.

#### Addressing Flagged Content in Twenty-Four Hours

A central obligation that would be created by the new legislation is that content that falls within the five categories of harmful content would have to be made inaccessible to Canadians within twenty-four hours of being flagged. This twenty-four-timeline is, in different senses, both too fast and too slow. It is too fast for platforms to make good decisions about whether or not the content in question meets the definitions of the five types of prohibited content, especially hate speech or incitements to violence. But it is also too slow to be of much help to those that are targeted by a sea of hateful content. While it may have a limited impact on harmful content as part of a multi-pronged strategy to reduce such content, the costs significantly outweigh the relatively small benefit.

#### This requirement will not significantly reduce designated content

The proposed requirement that platforms make flagged content that meets one of the five definitions of harmful content appears to be based on Germany's NetzDG (*Netzwerkdurchsetzungsgesetz*), with its similar twenty-four-hour timeline for addressing illegal content on social media platforms. However, that law <u>has not been able to quell the tide of hateful content</u>. This is not surprising. On large platforms like Facebook, the amount of content that must be dealt with is astronomical. Facebook's Transparency Report, for example, says that Facebook took 31.5 million content actions on hate speech alone in the second quarter of 2021. Addressing content quickly is difficult, but even if it is addressed within twenty-four hours, there is still a large window of time for people to come into contact with harmful content. This is especially true where dedicated malicious actors seek to flood a platform with such content. For them, a twenty-four-hour window is barely an imposition. As demonstrated by the recent "<u>hate raids</u>" on Twitch, it is often trivial for a small group of people to carry out rapid coordinated hate campaigns.

Platforms can and have developed tools to deal with such actors, including large-scale accountlevel actions, proactive monitoring for reposted content, and bot detection. But a requirement to Comments on the Government's proposed approach to address harmful content online

remove flagged content within twenty-four hours will do little for a significant amount of designated content.

Moreover, since the requirement to address designated content within twenty-four hours only applies to content that has been flagged under the proposed legislation, this will significantly limit the amount of hate speech that is subject to blocking. The problem with hate speech isn't merely its immediate and significant impacts upon those targeted by it, but its ability to radicalize those that may be susceptible to it. Within certain communities and friend groups, hate content is unlikely to be flagged. Here, too, the obligations will be of limited impact, and hate speech will continue to proliferate in communities where it currently does.

#### This requirement will stifle legitimate speech

Given the foregoing, one might then suggest that the proposed legislation simply does not go far enough in requiring platforms to take action on designated content. While it is certainly true that once could imagine more draconian regulation that would effectively mandate addressing all harmful content, it would do so at the expense of an enormous amount of legitimate expression. Indeed, the problem with the requirement to address content in twenty-four hours isn't that it will do *nothing*, but that it will not do enough to outweigh its costs to legitimate expression.

The core problem is that the combination of fast timelines for addressing content and significant potential penalties for non-compliance incentivizes over-blocking. The twenty-four-timeline does not provide sufficient time to make nuanced context-rich decisions about whether content meets the definitions contained in the proposed Act. For this reason, when faced with content that *is* flagged, reviewers will err on the side of caution, blocking content that might otherwise be found acceptable. Even the controversial German NetzDG contains provisions allowing for a longer review timeline in cases where the illegality of the content is not obvious.

Further, the combination of a flagging system that is liable to be abused by trolls and malicious actors and rapid content review requirements are likely to lead to over-blocking of content from vulnerable groups. We have already <u>witnessed the abuse</u> of the copyright take-down notices under the United States' Digital Millennium Copyright Act, and that legislation includes penalties for abusing the system. There is no reason to believe that the proposed flagging system will not be similarly abused, especially to target minorities and vulnerable groups. As with Twitch's hate raids, it is trivial for motivated actors to take a large number of malicious actions, which could include massive flagging campaigns, which would predictably lead to reviewers removing at least some of that content. While the Technical Paper attempts to limit this by requiring OCSPs to take measures to prevent discrimination, as mentioned, this is difficult in practice. Putting content reviewers under increasingly tight timelines for making decisions on content is only likely to exacerbate this problem, especially when combined with a flagging system that can be abused by bad actors and that incentivizes over-blocking.

Finally, laws that require expeditious actions on certain content also have the potential to embolden other illiberal countries around the world to impose censorship on internet intermediaries. We are already witnessing the rise of laws that require the rapid removal of flagged political criticism or the discussion of controversial topics online under the auspices of

Comments on the Government's proposed approach to address harmful content online

preventing abuse or misinformation, such as in <u>India</u> and <u>Thailand</u>. Canada should not put itself in the position of becoming an inspiration or justification for the creation of such laws internationally.

For these reasons, the obligation to address flagged content within twenty-four hours should be rejected.

#### **Mandatory Reporting to Law Enforcement**

Perhaps the most concerning aspect of the entire proposal is the prospect that the legislation will mandate that major platforms used by Canadians become functional arms of a surveillance state. The combination of general monitoring obligations and mandatory reporting to law enforcement or other agencies of information related to certain criminal offences raises enormous privacy concerns for Canadians.

Neither of the options contemplated in paragraph 20 of the Technical Paper should be combined in any way with mandatory general monitoring obligations. Of the two options, only the first option, which contemplates reporting only in cases where there are reasonable grounds to suspect that the harmful content reflects an imminent risk of serious harm, is defensible, and only where such content has been expressly flagged to the platform. The other option would effectively force platforms to report to police whenever their own rapid and imperfect assessments identified content as potentially related to a prescribed offence. This would lead to significant amounts of over-reporting in what would amount to an effective police dragnet. The potential for adverse privacy and data protection breaches is enormous.

In any case, no obligations concerning reporting to law enforcement should be imposed without significant additional consultation with stakeholders, privacy experts, and regulators, including the Privacy Commissioner of Canada.

#### Conclusion

I have not addressed a number of issues contained in the proposal, including the creation of the Digital Safety Commission of Canada, the Digital Recourse Council, the Digital Safety Commissioner of Canada, and the Advisory Board. In my view, there is no reason to address these given that the overarching regulatory scheme in which they would operate, and the platform obligations they would enforce and oversee, are fundamentally flawed. The existence of such bodies should only be contemplated within a new, more carefully considered legislative package.

Such a package should also address aspects of the online ecosystem that are not currently considered and aim to increase the degree of democratic accountability of platforms. The vast majority of content moderation decisions made by platforms will be unaffected by the proposed regulations. This includes decisions related to content that falls outside of the designated categories, as well as decisions to remove content, especially content created or posted by vulnerable groups. It also leaves out all algorithmic ranking and recommendation systems, and does not address other modes of taking action on content, from account-level actions to content labelling. Indeed, under the proposed regulations, even where the Digital Recourse Council

#### Englishma connormation ann ann a Iollan ann am 22 à Tallannaí an Ean annsaí raisseoir ann an an Bhe Accept ag annsaí annsaí

#### Matthew Marinett

Comments on the Government's proposed approach to address harmful content online

determines a piece of content to not be violating the proposed regulations, the platform is still able to deal with the content as it sees fit under its own policies. And this is to say nothing about how platforms design and implement their policies and systems. In other words, in focusing only on ensuring that a few limited categories of harmful content are rendered inaccessible to Canadians, the governance structure of platforms and their role in moderating the information ecosystem are not affected.

This is not to say that there is no scope for regulation aimed at reducing harm on social media platforms. But regulation needs to understand that simple mandates that demand that platforms take specific content moderation actions or face consequences are unlikely to succeed.

Instead, regulation should focus on ensuring that content moderation processes are transparent, effective, and fair and that companies engage in risk assessments and regular internal audits to ensure that their policies and enforcement respect human rights and human dignity. Regulators should work with platforms to set platform-wide harm-reduction goals based on clear criteria backed by regular audits and mandatory transparency, rather than taking an approach based on unworkable general monitoring obligations or based on the rapid review of whatever content happens to be flagged. In this way, some of the transparency requirements contemplated in paragraph 14 of the technical paper are laudable, but transparency should be aimed at overall harm reduction over time rather than being tied to specific content moderation approaches. Government officials do not know how to do content moderation. The role of government should be to set targets, not to tell platforms precisely how to meet them.

It remains my hope that the Government of Canada can become a leader in social media and internet intermediary regulation by carefully developing a true made-in-Canada approach. Unfortunately, this proposal fails to live up to that hope. There is little in the current proposal to be commended, and, in my view, the approach taken in the proposed legislation should be fundamentally reconsidered. I recommend that the Government start over through a robust consultation process drawing in experts, civil society, and other stakeholders in order to develop a regulatory regime that properly balances the interests of all and can actually result in real harm reduction while also improving democratic control of our information environment.

Sincerely,

Matthew Marinett Doctoral Candidate University of Toronto, Faculty of Law matthew.marinett@utoronto.ca

September 2021



Pinterest welcomes the opportunity to share our views with the Department of Canadian Heritage (DCH) on its proposed framework for an Act of Parliament, and to explain our perspective as a mid-sized platform committed to effective content moderation and the safety of our users. We support efforts in Canada, and around the world, to adopt sound regulations for Internet platforms and technologies.

In short, we share many of the concerns raised by experts across civil society, industry and academia about the current draft of this proposal. We appreciate that this proposal was motivated by a genuine interest in making the Internet safer, something we have a strong self-interest in doing as well. Our concern is that this proposal will have the unintended consequence of making that ultimate goal more difficult to achieve.

#### Introduction to Pinterest

People come to Pinterest to find inspiration for their lives, including recipes, home and style ideas, travel destinations and more. People save these ideas – which we call Pins – into collections, which we call boards. Many Pins come directly from businesses and publishers, which upload their own content for people who visit Pinterest (Pinners) to discover and save. The vast majority of those ideas are positive and inspiring, and our goal is for people to view Pinterest as a place where they can focus on themselves, their interests and their aspirations. What we hear from Pinners reinforces that: 91% of Pinners say that Pinterest is filled with positivity, and 89% say that they leave Pinterest feeling empowered<sup>[1]</sup>. In this way, Pinterest is personal media – not social media – that people use to curate ideas for themselves and their own lives.

#### Our approach to content moderation

While Pinners do not generally turn to Pinterest as a place to share dangerous or offensive material, or even to share political commentary and other typical varieties of "viral" content, we recognize that it's hard to feel inspired if you don't feel safe.

Being a platform for personal inspiration means being deliberate about the type of inspiration we want people to find. It also means being thoughtful about what we do not want people to find. For example, Pinterest was one of the first companies to disallow political campaign ads. We were also one of the first to disallow harmful misinformation, like the promotion of false cures and anti-vaccination content. More relevant to this proposal in Canada, our guidelines prohibit content in the five categories listed in DCH's proposal, including policies against

hateful activities, sexually exploitative content, violent extremist content, and much more. Our rules often sweep more broadly than the law, prohibiting material that may be legal but that undermines our mission and the health of the Pinterest community.

We also recognize that rules are a first step. We employ a dedicated team to enforce these rules, and actively work to develop technical tools to help them identify and act against content that violates our policies. One way we identify content is with the help of user reports, although our hope is that people won't encounter this type of content in the first place. Thankfully, as we shared in <u>our latest Transparency Report</u>, in Q4 2020 less than 0.02% of monthly active users reported Pins which were confirmed to violate our content policy. In the same period, 85% of medical misinformation content was removed before any users saw it. For adult content in that period, we estimate that 98% of content that was removed on Pinterest was seen by fewer than 100 people.

Pinterest's content policies, moderation practices, and tools have evolved in response to technical and societal developments, as well as the needs of our users. For example, in 2017, we developed our policy against health misinformation on Pinterest, including anti-vax content. Building on an earlier effort in 2019, last year we customised the results users see when they search for information related to the ongoing COVID-19 public health crisis. In order to prevent people from encountering harmful health misinformation, results for queries related to the COVID-19 pandemic now show only content from leading public health institutions like the World Health Organisation and National Health Service.

Although we are relatively small in size – employing some 2,700 people, by contrast to the tens of thousands employed by our larger peer companies – we take pride in the high standards we set for both content policy development and enforcement.

#### Our views on the proposed framework

We support regulation to address online harms, including regulation that shapes platforms' content moderation practices. We have concerns about this proposed framework, however, which we have outlined below.

#### **User Rights**

Pinterest is not a place for politics and we are not focused on fostering free expression. However, several provisions of the proposed law may have implications for the rights and interests of law-abiding Internet users which we think deserves more discussion. The requirement to take down unlawful content on 24-hours notice, for example, will provide many small or medium-sized platforms with little time to assess potentially complex legal claims. The strong incentive will be to simply take down any content that is alleged to violate the law, in order to avoid legal risk. Platform companies of all sizes regularly receive abusive or mistaken demands to remove lawful and even societally important content. At Pinterest, we do our best to identify and resist such improper requests. But the largest companies will be uniquely positioned to carry out the kind of rapid-yet-accurate legal analysis that the proposed law suggests.

Similarly, the requirement that platforms "take all reasonable measures, which can include the use of automated systems, to identify harmful content" may, in practice, incentivize smaller platforms to rely on imprecise filtering tools. Legal mandates to adopt poorly-defined or understood automated systems create serious risk of harm to users.

Finally, while we have a lower volume of law enforcement requests than many of our larger peers, we share the concerns expressed by industry, civil society and academic experts about the proposal's broad mandate to report users to law enforcement. At Pinterest, we do report dangerously unlawful activity in accordance with our <u>law enforcement guidelines</u>. At the same time, we also recognize that people will only use our service if we continue to earn their trust. A law compelling Internet platforms to adopt a novel and broadly defined reporting role may undermine that trust.

#### Improving clarity and scope

Some of the challenges with this proposal stem from reasonable ideas - such as offering users a chance to appeal takedown decisions - that are poorly defined. The proposal allows government actors to disregard allegations that are "frivolous, trivial, vexatious, [or] made in bad faith," for example, but grants no such leeway to companies themselves. Similarly, it seems to require platforms to terminate a user's control over her own content and data from the moment that her "content is identified or flagged as prescribed" - with no regard to the legitimacy of the accusation. It also proposes transparency measures that, as currently worded, may be difficult to achieve - such as identifying the overall "volume and type of harmful content" on the entire platform, rather than the volume that has been identified through content moderation efforts. These imprecisely designed operational mechanics are coupled with sweeping powers for the Digital Safety Commissioner, who may order a platform to do "any act or thing" the Commissioner believes may be required to ensure legal compliance. Inspectors may also enter "any place" where they reasonably believe they may find "any document, information or any other thing, including computer algorithms and software, relevant to the purpose of verifying compliance and preventing non-compliance." All platforms, but particularly startups and scale-ups assessing legal risks and protections, would benefit from more clarity in all of these examples, among others.

## Comprehensively addressing harmful content

Aside from collaboration between more mature platforms on certain types of content, the approach, sophistication and technical resources a given company may invest in moderating content can vary. Rules designed with the very largest companies in mind may not address a particular challenge holistically, instead sending that content to other, smaller platforms that may not be in scope or may be less inclined towards taking a responsible approach. It may also have the unintended consequence of further entrenching the largest platforms, and turning what should be a shared interest into a competitive advantage. To help address this, we would recommend integrating proportionality throughout the proposal, assessing systemic risk based on the nature of a platform, usage patterns, notices received per year on illegal content, or measures taken by the online platform to mitigate those risks.

## Conclusion

Pinterest opened its Canada office in 2018 and recently announced that Toronto would be our first international engineering hub outside the U.S. We are grateful for the estimated 13 million people in Canada who visit Pinterest each month to find inspiring ideas and look forward to continuing this investment and growth in Canada.

We appreciate this opportunity to share our views on this proposal and would be happy to continue our engagement with the Department of Canadian Heritage on this important issue.



121 HEATLEY AVENUE VANCOUVER; B.C. V6A 3E9 CANADA T 604.255.9700 F 604.255.1552 pivotlegal.org

equality lifts everyone

#### Submissions regarding the Federal Government's Proposed Approach to Address Harmful Content Online

We write regarding Canada's proposed regulatory framework for addressing certain types of 'harmful online content'.<sup>1</sup> Our submissions focus on the harms this overly broad new legal regime would cause to sex workers, whose livelihoods would be harmed and legal rights infringed.

#### About Pivot Legal Society

Founded in 2001, Pivot Legal Society is a non-profit organization that works in partnership with communities affected by poverty and social exclusion to identify priorities and develop solutions to complex human rights issues. As an organization based in the Downtown Eastside, we work on the stolen lands of the xwma0kwayam (Musqueam), Skwxwú7mesh (Squamish), and Salílwata?/Selilwitulh (Tsleil-Waututh) peoples.

Pivot's work is focused in four policy areas: police accountability, drug policy, homelessness, and sex workers' rights.

#### Concerns about the Government's Proposed Framework

Our submissions focus on the sexually-related-content restrictions found in the Proposed Framework. In solidarity with sex workers and sex worker-led groups across Canada, we are particularly concerned about three aspects of the new laws:

- a) the demand for proactive monitoring, aka filtering, by website service providers;
- b) websites' obligation to quickly remove suspected harmful content; and
- c) the requirement that service providers report content to the police.

We will address each of these aspects of the new regime in turn.

a) The demand for proactive monitoring, aka filtering, by website service providers

Under the Proposed Framework, online communication service providers (Facebook, Twitter, etc) would be legally required to "take all reasonable measures, which can include the use of automated systems, to identify harmful content"<sup>2</sup>, imposing an obligation to proactively monitor, or filter, user content, including with artificial intelligence (AI). This is an invasive and flawed system that will further surveil and stigmatize sex workers. Automated systems would likely capture sexual content that has been generated by adult, consenting sex workers.

<sup>&</sup>lt;sup>1</sup> Harmful content is defined as child sexual exploitation; terrorist content; content that incites violence; hate speech; and the non-consensual sharing of intimate images: Government of Canada Technical Paper at Module 1(A), para 8. The Technical Paper is available at https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html

<sup>&</sup>lt;sup>2</sup> Technical Paper at Module 1(B), para 10

<sup>1</sup> Pice of the uncerted lembery of the Coast Salish Peoples, including the territories of the symalle-again (Marganium), Skwxw07mesh (Squamiet), and selfavera?i (Tetel-Wauluh) Mitton:

Al and moderation systems are systemically biased and given the stigma imposed on sex workers, there is every reason to believe these systems would disproportionately target and remove content from sex workers, especially those with intersecting identities such as racialized, disabled and queer sex workers. Reporting done by Carleton University academics describes how Al and moderation systems are "easily disposed to error and can impose bias on a colossal systemic scale"<sup>3</sup> and a recent academic article describes how "throughout the social media ecosystem, nonnormative and LGBTQ+ sexual expression is disproportionately taken down, restricted, and banned."<sup>4</sup>

Though complaint-based systems are also flawed, legally requiring service providers to comb their users' data for potentially harmful content is an overbroad regulation that will impact sex workers' legal right to advertise and provide their sexual services. Filtering has been opposed by human rights and civil society organizations around the world.<sup>5</sup>

### b) Websites' obligation to quickly remove suspected harmful content

The Proposed Framework demands that 'harmful content' is removed within 24 hours of being flagged (or some other time period – potentially shorter – imposed by regulation).<sup>6</sup>

Fear of liability means that platforms will likely err on the side of caution and remove *lawful* content. Given the very broad categories of content within the draft framework, it is highly likely that content will be swept up in service providers' rush to avoid extremely harsh financial penalties under the proposed laws (fines of 3% of global revenue or \$10 million, whichever is more<sup>7</sup>). Platforms may also want to avoid risk by enacting broad Terms of Service that prohibit types of legal speech and content. Given the current, misplaced conflation of sex work with human trafficking for the purposes of sexual exploitation, sexual content would be an obvious target for restrictions and removal. Simply put, stigma against sex work and the conflation of sex work with trafficking would be baked into any filtering system.

Due to police interference and harassment, as well as the COVID-19 pandemic, many sex workers use online platforms as safer or more accessible places for work and advertising. Incentivizing rapid online content removal will hurt their work and expose them to greater danger.

## c) The requirement that service providers report content to the police

The Proposed Framework requires some form of mandatory reporting of so-called harmful content by service providers to law enforcement. The Framework sets out two potential regimes for reporting:

<sup>&</sup>lt;sup>3</sup> Merlyna Lim and Ghadah Alrasheed, "Beyond a technical bug: Biased algorithms and moderation are censoring activists on social media" (May 16, 2021), available at <a href="https://newsroom.carleton.ca/story/biased-algorithms-moderation-censoring-activists/">https://newsroom.carleton.ca/story/biased-algorithms-moderation-censoring-activists/</a>

<sup>&</sup>lt;sup>4</sup> Ari Ezra Waldman, "Disorderly Conduct", available online at https://papers.ssrn.com/sol3/papers.cfm?abstract\_ld=3906001

<sup>&</sup>lt;sup>5</sup> See for example, the Civil Society Letter to the European Parliament about Proposed Regulation on Preventing the Dissemination of Terrorist Content Online found here: <u>https://cdt.org/wp-content/uploads/2019/02/Civil-Society-Letter-to-European-Parliament-on-Terrorism-Database.pdf</u>

<sup>&</sup>lt;sup>6</sup> Technical Paper at Module 1(B), para 11 (a) and (b)

<sup>&</sup>lt;sup>7</sup> Technical Paper at Module 1(D), para 108

Option 1: service providers report to law enforcement when there are "reasonable grounds to suspect that [harmful content] reflects an **imminent risk** of serious harm to any person or to property";<sup>8</sup> or

Option 2: service providers report **all harmful content** to law enforcement when a legal threshold (to be decided by regulation) is met. That threshold could be a "reasonable suspicion" or "reasonable grounds to believe" that something is 'harmful content'.<sup>9</sup>

Sex workers are already overpoliced, surveilled and harassed. The proposed laws requiring reporting to police, especially Option 2, would further entrench and expand police powers and cause very real harm to sex workers. A police record, and potential investigation, can have many consequences (for example, in child protection matters, and in criminal record checks for volunteering and employment positions). Under the Proposed Framework, a person may not even know that their content has been reported to police.<sup>10</sup>

We know that sex workers are already harmed by overpolicing and criminalization. We also know that policing disproportionately targets and harms BIPOC communities, a fact recognized by the Supreme Court of Canada: "[w]e do not hesitate to find that... we have arrived at a place where the research now shows disproportionate policing of racialized and low-income communities".<sup>11</sup>

The Proposed Framework's massive expansion of police involvement is all the more unreasonable because it could well be based on an AI or moderation decision made extremely quickly. As Michael Geist, a legal scholar specializing in digital regulation, summarized the problem: there is "the prospect of an AI identifying what it thinks is content caught by the law and generating a report to the RCMP."<sup>12</sup> In other words, there is the "possibility of Canadians garnering police records over posts that a machine thought was captured by the law."<sup>13</sup>

#### Conclusion

The Proposed Framework would infringe sex workers' ability to find and perform work, during a global pandemic that has eroded sex workers' ability to earn money while they are simultaneously excluded from many government supports. Imperfect website filters and the conscious or unconscious bias of platforms' human content moderators, combined with harsh penalties for not removing content, will lead to service providers erring on the safe side and removing large swaths of sexual content. This will have a negative impact on sex workers, and particularly on those with intersecting marginalized identities.

<sup>&</sup>lt;sup>8</sup> Technical Paper at Module 1(B), para 20(a)

<sup>&</sup>lt;sup>9</sup> Technical Paper at Module 1(B), para 20(b); and Government of Canada Discussion Guide, under "Engaging law enforcement and CSIS". The Discussion Guide is available at <u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-</u> content/discussion-guide.html

<sup>10</sup> Technical Paper at Module 1(B), paras 26 and 27

<sup>&</sup>lt;sup>11</sup> R. v. Le, 2019 SCC 34 at para. 97

<sup>&</sup>lt;sup>12</sup> Michael Geist, "Picking Up Where Bill C-10 Left Off: The Canadian Government's Non-Consultation on Online Harms Legislation" (July 30, 2021), available at <a href="https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/">https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/</a> ["Geist Article"]

<sup>&</sup>lt;sup>13</sup> Geist Article

In addition to the issues outlined above, commentators have raised other serious concerns about the proposed laws.<sup>14</sup> These include concerns about the creation of new regulatory bodies with expansive powers, including the power to inspect any platform's premises to examine any data in their computer systems, and the ability to block access to a website throughout Canada.

Any laws and regulations arising out of the Proposed Framework must be grounded in the needs of, and avoid harm to, sex workers. In its current form, the laws are overly broad and will infringe sex workers' constitutional and human rights.

<sup>&</sup>lt;sup>14</sup> See, for example, Darryl Carmichael and Emily Laidlaw, "The Federal's Government's Proposal to Address Online Harms: Explanation and Critique" (September 13, 2021), available at: <u>https://ablawg.ca/2021/09/13/the-federal-governments-proposal-to-address-online-harms-explanation-and-critique</u>; Mat Hatfield, "A first look at Canada's harmful content proposal" (September 22, 2021), available at: <u>https://openmedia.org/article/item/a-first-look-at-canadas-harmful-content-proposal;</u> and Daphne Keller, "Five Big Problems with Canada's Proposed Regulatory Framework for 'Harmful Online Content'" (August 31, 2021), available at: <u>https://techpolicy.press/five-big-problems-with-canadas-proposed-regulatory-framework-for-harmful-online-content/</u>

## Government of Canada Consultation on the Proposed Approach to Address

## Harmful Content Online

Submission by

Professor Michael Geist

Canada Research Chair in Internet and E-commerce Law

University of Ottawa, Faculty of Law

Centre for Law, Technology and Society

September 2021

#### A. Overview

I am a law professor at the University of Ottawa where I hold the Canada Research Chair in Internet and E-commerce Law and serve as a member of the Centre for Law, Technology and Society. I focus on the intersection between law and technology with an emphasis on digital policies. I submit these comments in a personal capacity representing only my own views.

My submission raises serious concerns with the government's proposed approach. I raise many specific concerns, but there are eight general comments that need to be raised.

- The proposed approach does not strike an appropriate balance between addressing online harms and safeguarding freedom of expression. Indeed, after a single perfunctory statement on the benefits of Online Communications Services (OCSs) which says little about the benefits of freedom of expression, the document does not include a single mention of the Charter of Rights and Freedoms or net neutrality. There is surely a need to address online harms, but doing so must be Charter compliant and consistent with Canadian values of freedom of expression. I believe the proposed approach fails to adequately account for the freedom of expression side of the ledger.
- 2. Rather than adopting a "made in Canada" approach consistent with Canadian values, the plan relies heavily on policy developments elsewhere. Yet the reality is that those models from countries such as France, Germany, and Australia have met with strong opposition and raised serious concerns of unintended consequences. Indeed, France's approach has been ruled unconstitutional, Germany's model has resulted in over-broad removal of lawful content and a lack of due process, and Australia's framework is entirely unproven. An evidence-based approach would better account for these experiences rather than seek to mirror them.
- 3. The proposed approach mistakenly treats a series of harms spreading hateful content, propaganda, violence, sexual exploitation of children, and non-consensual distribution of intimate images as equivalent and requiring the same legislative and regulatory response. While there is a commonality between these harms as so-called "illegal speech", there are also significant differences. For example, it makes no sense to treat online hate as the equivalent of child pornography. By prescribing the same approach for all these forms of content, the efficacy of the policy is called into question.
- 4. There are lingering concerns about scope-creep with this proposal. Government officials have previously referenced the need to address "harmful" or "hurtful" comments, raising the prospect of expanding the model far beyond the current five forms of illegal speech cited in the proposal. Moreover, the government has indicated that these rules apply only to OCSs, identifying Facebook, Youtube, TikTok, Instagram, and Twitter as examples. It notes that there will be an exception for private communications and telecommunications such as wireless companies, Skype and WhatsApp (along with products and services such as TripAdvisor that are not OCSs). Yet during a briefing with stakeholders, officials were asked why the law shouldn't be extended to private communications on platforms as well, noting that these harms may occur on private messaging. Given that the government previously provided assurances of the exclusion of user generated content in Bill C-10

only to backtrack and make it subject to CRTC regulation, there is a need for renewed assurances about the scope of the rules.

- 5. The proposed approach envisions a massive new bureaucratic super-structure to oversee online harms and Internet based services. Due process concerns dictate that there be a suitable administrative structure to address these issues. However, some of the proposed models are ill-conceived that will not scale well nor afford the much-needed due process. For example, adjudicating over potentially tens of thousands of content cases is unworkable and would require massive resources with real questions about the appropriate oversight. Similarly, the powers associated with investigations are enormously problematic with serious implications for freedom of the press and freedom of expression.
- 6. The proposed approach threatens Canada's important role as a model for the rest of the world. Some of the proposals risk being deployed by autocratic countries to suppress freedom of expression with Canada cited as an example for why such measures are reasonable. The government should be asking a simple question with respect to many of its proposals: would Canadians be comfortable with the same measures being implemented countries such as China, Saudi Arabia, or Iran. If the answer is no (as I argue it should be), the government should think twice before risking its reputation as a leader in freedom of expression.
- 7. The proposed approach also threatens to harm the very groups it purports to protect. Without full due process and with clear incentives to remove content, there are real fears that the rules will be used to target BIPOC communities and vulnerable groups. Those groups could be silenced by a process that is weaponized by purveyors of hate with their voices removed due to poorly conceived rules that do not feature adequate due process.
- 8. During the last election campaign, the government promised to move forward within 100 days of its mandate. Given that commitment as well as the structure of the consultation that reads more like a legislative outline rather than a genuine attempt to solicit feedback there are considerable doubts about this consultative process. Consultations should not be a box-ticking exercise in which the actual responses are not fully factored into policy decisions. The challenge of reading, processing, analyzing and ultimately incorporating consultation responses within a three month period appears entirely unrealistic. The government should provide assurances that there will be no legislation without taking the consultation responses fully into account.

#### B. Specific Concerns

#### 1. 24 Hour Takedowns

The proposed approach includes a requirement for OCSs to implement measures to identify harmful content and to respond to any content flagged by any user within 24 hours. The OCSs would be required to either identify the content as harmful and remove it or respond by concluding that it is not harmful. The OCSs can seek assistance from the new Digital Safety Commissioner on content moderation issues. The proposed legislation would then incorporate a wide range of reporting requirements, some of which would be subject to confidentiality restrictions, so the companies would be precluded from notifying affected individuals.

By mandating such rapid takedowns of content, there is a clear risk of over-removal of content since it is difficult to give the content a proper assessment to understand its context. Furthermore, since many companies will use automatic systems to meet their legal obligations, experience elsewhere suggests that there will be significant over-removal of otherwise lawful content.<sup>1</sup>

a. Germany

The proposed approach appears largely modeled on the German *NetzDG* law. The German approach sparked international criticism stating with fears it would seriously harm free speech when it was adopted. It imposes a 24-hour time limit to remove obviously illegal content and allowed for up to 7 days to make a decision in circumstances where it is not clearly illegal – where an argument could be made that it was legal. This provides more nuance than the Canadian model.<sup>2</sup>

Since enactment, the German experience has demonstrably been shown to lead to over-removal of content as Internet services respond to high penalties by erring on the side of content removal.<sup>3</sup> For example, In 2018, Facebook took down a picture of a traffic sign with a bikini top on it from both Facebook and Instagram. The picture was created by an anonymous artist whose work consists of humorous and politically pointed alterations to public signs – they have won awards for their work.<sup>4</sup>

That same year, Twitter blocked the account of the satirical magazine *Titanic*, after they published a tweet parodying the far-right populist Alternative for Germany (AfD) party's Islamophobia. The tweet pretended to be coming from a leading AfD politician complaining about German police using Arabic numerals, which are of course standard throughout the west. Again, critics pointed to this as showing that NetzDG is over-blocking because something this clearly satirical was taken down.<sup>5</sup>

A large part of the problem with a 24 hour takedown requirement is that it does not allow for a fulsome analysis of edge cases. For example, in July 2018 YouTube and Twitter presented their first transparency reports for the first half of 2018 with the law. In YouTube's case, it received hundreds of thousands of takedown requests, but found only 27% justified such action. Further,

<sup>&</sup>lt;sup>1</sup> Daphne Keller, "Empirical Evidence of Over-Removal By Internet Companies Under Intermediary Liability Laws: An Updated List" (February 8, 2021) online: *Stanford Center for Internet and Society* 

<sup>&</sup>lt;http://cyberlaw.stanford.edu/blog/2021/02/empirical-evidence-over-removal-internet-companies-underintermediary-liability-laws>

<sup>&</sup>lt;sup>2</sup> Darryl Carmichael & Emily Laidlaw, "The Federal Government's Proposal to Address Online Harms: Explanation and Critique" (September 13, 2021) online: *ABlawg* <a href="https://ablawg.ca/2021/09/13/the-federal-governments-proposal-to-address-online-harms-explanation-and-critique">https://ablawg.ca/2021/09/13/the-federal-governments-proposal-to-address-online-harms-explanation-and-critique</a>

<sup>&</sup>lt;sup>3</sup> Svea Windwehr & Jillian C York, "Turkey's New Internet Law Is the Worst Version of Germany's NetzDG Yet" (July 30, 2020) online: *EFF* <a href="https://www.eff.org/deeplinks/2020/07/turkeys-new-internet-law-worst-version-germanys-netzdg-yet">https://www.eff.org/deeplinks/2020/07/turkeys-new-internet-law-worst-version-germanys-netzdg-yet</a>

<sup>&</sup>lt;sup>4</sup> Jefferson Chase, "Facebook slammed for censoring German street artist" (January 15, 2018) online: DW

<sup>&</sup>lt;https://www.dw.com/en/facebook-slammed-for-censoring-german-street-artist/a-4215521>,

<sup>&</sup>lt;sup>5</sup> Ibid.

hundreds of cases required more than a week to reach a determination and dozens required external counsel to provide assistance.<sup>6</sup> Meanwhile, Twitter found that only 11% of takedown requests were justified and also reported that hundreds required more than 24 hours to reach a determination.<sup>7</sup> The lesson is clear: trading expediency for due process and careful examination of takedown claims invariably leads to over-removal of lawful content.

## b. France

France has also endeavoured to establish rapid takedowns. In May 2020, it adopted a controversial online hate speech bill, known as the *Avia Bill* that required social media platforms and search engines to remove flagged hateful content within 24 hours and flagged terrorist propaganda and child sexual abuse material within one hour. Failure led to the threat of high fines.<sup>8</sup>

While the law may have influenced the proposed Canadian approach, it is important to note that it was struck down by the French Constitutional Court as unconstitutional. The court ruled that the 24-hour time window was "particularly brief"<sup>9</sup> and that this time limit to take down "manifestly illicit" online posts "could only encourage operators of online platforms to remove content that's flagged to them, whether or not it's manifestly illicit". Further, it concluded that the law constituted "an infringement of the right to free expression and communication that isn't necessary, appropriate and proportionate".<sup>10</sup> It also struck down the one-hour limit on taking down content deemed child pornography or terrorist content. Finally, in a statement, the court said that "freedom of expression and communication is all the more precious since its exercise is a condition of democracy and one of the guarantees of respect for other rights and freedoms."<sup>11</sup>

c. United States

In 2017, the United States passed the *Allow States and Victims to Fight Online Sex Trafficking Act* (FOSTA) intending to penalize sites that hosted speech related to child sexual abuse and trafficking. This is somewhat different than the online harms legislation in Germany and France because it has a far narrower scope. However, the law had the similar impact, leading to large and small Internet platforms censoring broad swaths of speech that contained adult content. This

<sup>&</sup>lt;sup>6</sup> Thomas Wischmeyer, "What is illegal offline is also illegal online': the German Network Enforcement Act 2017" in Bilyana Petkova & Tuomas Ojanen, eds, *Fundamental Rights Protection Online* (Cheltenham: Edward Elgar Publishing Limited, 2020) 28 at 54.

<sup>7</sup> Ibid.

<sup>&</sup>lt;sup>8</sup> Laura Kayali, "France gives final green light to law cracking down on hate speech online" (May 13, 2020) online: *Politico* <a href="https://www.politico.eu/article/france-gives-final-green-light-to-law-cracking-down-on-hate-speech-online/">https://www.politico.eu/article/france-gives-final-green-light-to-law-cracking-down-on-hate-speech-online/</a>>

<sup>&</sup>lt;sup>9</sup> Mathieu Rosemain, "France's top court rejects core of law targeting online hate speech" (June 18, 2020) online: *Reuters* <a href="https://www.reuters.com/article/us-france-tech-regulation/frances-top-court-rejects-core-of-law-targeting-online-hate-speech-idUSKBN23P32O">https://www.reuters.com/article/us-france-tech-regulation/frances-top-court-rejects-core-of-law-targeting-online-hate-speech-idUSKBN23P32O</a>>

<sup>&</sup>lt;sup>10</sup> Sam Schechner, "French Court Strikes Down Core of New Hate-Speech Law" (June 18, 2020) online: *Wall Street Journal* <a href="https://www-proquest-">https://www-proquest-</a>

com.proxy.bib.uottawa.ca/docview/2414465405/ADD9B3730D7B4A0FPQ/2?accountid=14701>

<sup>&</sup>lt;sup>11</sup> Asia News Monitor, "France: French constitutional court blocks large portion of online hate speech law" (June 22, 2020) online: Asia News Monitor <a href="https://www-proquest-">https://www-proquest-</a>

com.proxy.bib.uottawa.ca/docview/2414779631/65AA1F6DFD404946PQ/3?accountid=14701>

had devastating consequences for marginalized communities and those that served them, especially organizations that provide support and services to victims of trafficking and child abuse, sex workers, and groups/individuals promoting sexual freedom.<sup>12</sup>

Indeed, the law had particularly devastating consequences on already vulnerable sex workers. There had been a broad movement for sex workers to move online to better protect themselves from both the dangers of the job and from police harassment. The online setting provided online forums, client-screening capabilities, "bad date" lists, and other intra-community safety tips. Countless amounts of these sources were either taken down or had to charge significantly more in the wake of FOSTA. Ironically, the law has made the position of sex workers *more* precarious since it forces sex workers back "on the streets" or back to a pimp - and has led to significant financial instability for them.<sup>13</sup>

The proposed approach risks raising many of the same concerns and problems experienced elsewhere. To be clear, there is a need to establish a system for the removal of illegal content and OCSs should be expected to comply with those takedown rules. However, it is critical to ensure that takedown requirements adequately account for due process and contain essential freedom of expression safeguards. The government's proposed approach as articulated in the consultation does not meet that standard.

#### 2. Proactive Monitoring

The proposed approach envisions pro-active monitoring and reporting requirements that could have significant negative implications. For example, it calls for pro-active content monitoring of the five harms, granting the Digital Safety Commissioner the power to assess whether artificial intelligence tools used to identify illegal content are sufficient. Moreover, the OCSs would face mandatory reporting requirements of users to law enforcement, leading to the prospect of an AI identifying what it thinks is content caught by the law and generating a report to the police. This represents a huge increase in private enforcement and the possibility of Canadians garnering police records over posts that a machine thought was captured by the law. Given the risks outlined below associated with AI and bias, the risk of machine generated police reports is particularly pronounced for BIPOC communities.

The issue of proactive monitoring has been the subject of opinions from three UN Special Rapporteurs in the context of an Indian law focused on online content regulation (Special Rapporteurs for the promotion and protection of the right to freedom of opinion and expression; on the rights to freedom of peaceful assembly and of association; and on the right to privacy).<sup>14</sup> The Special Rapporteurs expressed concern about the obligations of companies to monitor and rapidly remove user-generated content, which they feared will likely undermine the right to

<sup>&</sup>lt;sup>12</sup> Corynne McSherry & Katitza Rodriguez, "O (No!) Canada: Fast-Moving Proposal Creates Filtering, Blocking and Reporting Rules – and Speech Police to Enforce Them" (August 10, 2021) online: *EFF* 

<sup>&</sup>lt;sup>13</sup> Danielle Blunt & Ariel Wolf, "Erased: The Impact of FOSTA-SESTA" online (PDF): *Hacking//Hustling* <a href="https://hackinghustling.org/wp-content/uploads/2020/01/HackingHustling-Erased.pdf">https://hackinghustling.org/wp-content/uploads/2020/01/HackingHustling-Erased.pdf</a>

<sup>&</sup>lt;sup>14</sup> Katitza Rodriquez & Kurt Opsahl, "India's Draconian Rules for Internet Platforms Threaten User Privacy and Undermine Encryption" (July 20, 2021) online: *EFF* <a href="https://www.eff.org/deeplinks/2021/07/indias-draconian-rules-internet-platforms-threaten-user-privacy-and-undermine">https://www.eff.org/deeplinks/2021/07/indias-draconian-rules-internet-platforms-threaten-user-privacy-and-undermine</a>

freedom of expression. They noted that intermediaries could over-comply with takedown requests to limit their liability and develop digital recognition-based content removal systems or automated tools to restrict content. They added that the programs are unlikely to accurately evaluate cultural contexts and identify illegitimate content. Moreover, they worried that the short deadlines, coupled with the potential criminal penalties, could lead service providers to remove legitimate expression as a precaution to avoid sanctions. The concerns mirror those arising from the Canadian government's proposed approach.

As the demand for content moderation has increased, especially through proactive monitoring provisions, companies have moved toward automated versions of monitoring flagged content – both to ensure the wellbeing of human moderators and to be able to do it quicker – but this poses a major risk to the freedom of expression online. Automated systems are not capable of consistently identifying content correctly. Human communication is complex and context-dependent. AI misses this. Reports have shown that automated process take down large amounts of legal speech, and if there is no appeals process then the speech stays down.<sup>15</sup>

Such automated process have been shown to disproportionately remove some content over others, penalizing Black, Indigenous and LGBTQ+ people.<sup>16</sup> Several studies have shown that AI models for processing hate speech were more likely to flag content from black Americans than white Americans. One study from researchers at the University of Washington<sup>17</sup> found that AI was 1.5 times more likely to flag tweets by black Americans over white Americans, and 2.2 times more likely to flag tweets written in African American English.<sup>18</sup> Another study<sup>19</sup> found similar evidence of substantial racial bias against black speech in five widely used academic data sets for studying hate speech – it totalled around 155,800 twitter posts.<sup>20</sup>

The risks associated with the proposed proactive monitoring approach cannot be overstated. The proposals risks over-removal of content and increased reliance on AI-based monitoring systems that raise significant concerns of bias. These policies are most likely to harm the very people that the policy purports to help.

<sup>&</sup>lt;sup>15</sup> Svea Windwehr & Jillian C York, "Facebook's Most Recent Transparency Report Demonstrates the Pitfalls of Automated Content Moderation" (October 8, 2020) online: *EFF* <a href="https://www.eff.org/deeplinks/2020/10/facebooks-most-recent-transparency-report-demonstrates-pitfalls-automated-content">https://www.eff.org/deeplinks/2020/10/facebooks-most-recent-transparency-report-demonstrates-pitfalls-automated-content</a>

<sup>&</sup>lt;sup>16</sup> Digital Rights Watch, "Explainer: The Online Safety Bill" (February 11, 2021) online: Digital Rights Watch <a href="https://digitalrightswatch.org.au/2021/02/11/explainer-the-online-safety-">https://digitalrightswatch.org.au/2021/02/11/explainer-the-online-safety-</a>

bill/#:~:text=The%20Online%20Safety%20Bill%20was%20introduced%20in%20December,scheme%2C%20to%2 0remove%20material%20that%20seriously%20harms%20adults%2C>

<sup>&</sup>lt;sup>17</sup> Maarten Sap et al, "The Risk of Racial Bias in Hate Speech Detection", (2019) *Proceedings of the 57<sup>th</sup> Annual Meeting of the Association for Computational Linguistics*, 1668

<sup>&</sup>lt;https://homes.cs.washington.edu/~msap/pdfs/sap2019risk.pdf>

<sup>&</sup>lt;sup>18</sup> Shirin Ghaffary, "The algorithms that detect hate speech online are biased against black people" (August 15, 2019) online: *Vox* <a href="https://www.vox.com/recode/2019/8/15/20806384/social-media-hate-speech-bias-black-african-american-facebook-twitter">https://www.vox.com/recode/2019/8/15/20806384/social-media-hate-speech-bias-black-african-american-facebook-twitter</a>

<sup>&</sup>lt;sup>19</sup> Thomas Davidson, Debasmita Bhattacharya & Ingmar Weber, "Racial Bias in Hate Speech and Abusive Language Detection Datasets" (2019), *Proceedings of the Third Workshop on Abusive Language* 25 <a href="https://arxiv.org/pdf/1905.12516.pdf">https://arxiv.org/pdf/1905.12516.pdf</a>

<sup>20</sup> Ghaffaray, supra note 18.

Providente extende d'arte anti-barden las resultas antis de la Parlamenta de 2000 mente a la construction de las 1010 mentes de construction de las s

#### 3. Website Blocking

If the OCS does not comply with the order to remove certain content, the proposed approach introduces the possibility of website blocking with orders that all Canadian Internet service providers block access to the online communications service. The implications of these provisions are enormous, raising the likelihood of creating a country-wide blocking infrastructure within all ISPs with the costs passed on to consumers in the form of higher Internet and wireless bills.

The government's approach may be modelled on the Australian *Online Safety Act*, which grants the eSafety Commissioner the power to issue a non-negotiable request that ISPs block domains, URLs, or IP addresses hosting 'seriously harmful content'. The Commissioner does not need to observe any requirements of procedural fairness for these requests. The notices cannot be longer than 3 months, but there is no limit to how many times they can be renewed.<sup>21</sup> The Australian Act passed both houses of the legislature on June 23, 2021 and received Royal Assent on July 23, 2021.<sup>22</sup> However, the eSafety Commissioner announced that the bill will not take effect until January 23, 2022.<sup>23</sup> At this stage, the effects and effectiveness of the Australian law remains unknown.

However, there are numerous concerns with website blocking, particularly a state-sanctioned approach as envisioned by the government's proposal. The danger of over-blocking legitimate websites raises serious freedom of expression concerns, particularly since experience suggests that over-blocking is a likely outcome of blocking systems. The Council of Europe Commissioner for Human Rights issued a report in 2014 on the rule of law on the Internet in the wider digital world, noting,

blocking is inherently likely to produce unintentional false positives (blocking sites with no prohibited material) and false negatives (when sites with prohibited material slip through the filter). From the point of view of freedom of expression, the most problematic is widespread over-blocking: the blocking of access to sites that are not in any way illegal, even by the standards supposedly applied.<sup>24</sup>

The costs associated with site blocking can run into the millions of dollars with significant investments in blocking technologies and services, employee time to implement blocking orders, and associated service issues. Website blocking orders applied broadly to the myriad ISPs in Canada would have an uneven impact: larger ISPs may find it easier to integrate blocking technologies and processes into existing systems (some already block child sexual abuse material), whereas hundreds of smaller ISPs would face significant new costs that would affect their marketplace competitiveness. In fact, larger ISPs might ultimately benefit from higher fees passed along to subscribers and reduced competition. By harming the competitiveness of many

<sup>22</sup> <https://www.aph.gov.au/Parliamentary\_Business/Bills\_Legislation/Bills\_Search\_Results/Result?bId=r6680> <sup>23</sup> eSafety Commissioner, "Online Safety Act 2021; Fact sheet" (July 2021) online (PDF): *eSafety Commissioner* 

<sup>&</sup>lt;sup>21</sup> Digital Rights Watch, supra note 16.

chttps://www.esafety.gov.au/sites/default/files/2021-07/Online%20Safety%20Act%20-%20Fact%20sheet.pdf>
<sup>24</sup> Council of Europe, Commissioner for Human Rights, The rule of law on the Internet and in the wider digital world, (2014) at 13, online: <rm.coe.int/16806da51c>

smaller providers, website blocking may jeopardize efforts to extend affordable Internet access to all Canadians.

#### 4. Enforcement

The proposed approach identifies several measures to ensure enforcement. These include providing the public with the ability to file complaints with the Digital Safety Commissioner. The new commissioner would be empowered to hold hearings on any issue, including noncompliance or anything that the Commissioner believes is in the public interest. The Digital Safety Commissioner would have broad powers to order the OCSs "to do any act or thing, or refrain from doing anything necessary to ensure compliance with any obligations imposed on the OCSP by or under the Act within the time specified in the order." Moreover, there would also be able to conduct inspections of companies at any time:

"The Act should provide that the Digital Safety Commissioner may conduct inspections of OCSPs at any time, on either a routine or ad hoc basis, further to complaints, evidence of noncompliance, or at the Digital Safety Commissioner's own discretion, for the OCSP's compliance with the Act, regulations, decisions and orders related to a regulated OCS."

In fact, the inspection power extends to anyone, not just OCSs, if there are reasonable grounds that there may be information related to software, algorithms, or anything else relevant to an investigation.

Should a company declines to take down content, the public can also file complaints with the new Digital Recourse Council of Canada. This regulatory body would have the power to rule that content be taken down. Hearings can be conducted in secret under certain circumstances. Layered on top of these two bodies is a Digital Safety Commission, which provides support to the Commissioner and the complaints tribunal.

These proposals raise several concerns. The broad inspection power is similar to that found in Australia, where the *Online Safety Act* provides the eSafety Commissioner with the power to obtain information about the identity of an end-user of a 'social media service', a 'relevant electronic service' or 'designated internet service'. It also provides the Commissioner with investigative powers, which includes a requirement that one provides "any documents in possession of the person that may contain relevant information".<sup>25</sup>

The risk of overbroad or overzealous enforcement is very real. For example, in Australia Digital Rights Watch has raised concerns that investigative powers could extend to encrypted services – 'relevant electronic service' includes email, instant messaging, SMS, and chat. They note that the Commissioner has already spoken out against encryption because it makes investigations into online child sexual abuse more difficult. If extended to this realm, it could place Canadians' privacy and security at risk. The breadth of the inspection power suggests that it could also extend to journalists (raising issues involving protecting sources and freedom of the press), Internet service providers (raising privacy concerns and telecom regulatory issues), and any other

<sup>&</sup>lt;sup>25</sup> Digital Rights Watch, supra note 16.

business or person with any link to the investigation. A far more circumscribed power with real oversight is needed.

There are also concerns about the potential caseload and the ability for the Digital Recourse Council of Canada to provide fulsome review with appropriate due process. If claims run into the thousands, the system will simply not scale in a manner commensurate with demands. While that points to the challenges of moderating online content, a different system that better accounts for the likely demands is required.

hanstanten estenden tij beden beseten Konne av een beer bij betraak van Konne paal verkeer verken er onder op Die die ester de onderstaak



Submission for the Government of Canada's Proposed Approach to Combat Online Harms

FEDERATION OF

BLACK FÉDÉRATION DES CANADIANS CANADIENS

NOIRS

September 20th, 2021

Dear submission committee,

Thank you for the opportunity to submit comments regarding the Government of Canada's proposed online harms legislation.

<u>The Federation of Black Canadians</u> (FBC) is a national, non-profit organization, driven by organizations across the country that advances the social, economic, political and cultural interests of Canadians of African descent.

FBC acknowledges that we are currently in a hate crime crisis. 1 in 5 Canadians has experienced online hate and we want to advocate for members of our community most affected by this (<u>https://www.antihate.ca/the\_anti\_hate\_election\_report\_card</u>). As one of our five standing pillars is addressing anti-Black racism, we prioritize the elimination of all forms of discrimination against our community in order to build a stronger foundation for our youth, families and communities.

We do recognize that freedom of expression is a fundamental right in Canada but this right cannot be used to infringe on the [digital] safety and well-being of others and especially not marginalized groups such as our own. Therefore, online hate is of great concern for the FBC and we want to ensure an appropriate legislation that can address this grave issue.

The rise of hate crimes in Canada matched with the level of online hate that goes unaddressed and eventually, inconsequential is why we want to submit recommendations in lieu of a call to action.

FBC welcomes many aspects of the government's proposal such as the independent regulatory regime, annual reports, and other accountability measures that can hopefully be impactful.

While we welcome the Government's proposal, we respectfully submit the following recommendations for your consideration:

 We implore the government to collaborate with social media platforms to create stringent rules and regulations to proactively remove online hate. Social media platforms must be compelled by the government to have a stronger legal duty against online hate. If a monitoring mechanism is put in place to verify whether social media platforms are compliant with existing legislation that can facilitate accountability and transparency. We recommend that social media platforms be leveraged for public awareness campaigns as well that can address online hate. The

Electronical control completion services la Esti and control a l'Information Discontrol information and the the Access in constraints with



FEDERATION OF BLACK FÉDÉRATION DES CANADIANS CANADIENS NOIRS

enforcement of regulations as well as public education can create more sustainable change and impact on the issue of online hate.

- Consistent and robust consultation with marginalized communities and groups (such as our own) that are most disproportionately affected by online hate. This can develop to a working group that are adequately compensated and tasked with creating strategies to counter online hate. We believe that lived experience is a valid form of knowledge that can help inform policy, research, and implementation.
- There needs to be disciplinary measures implemented in order to address online hate, violence inciting, and misinformation. There are already existing laws and policies against online hate and incitement but there needs to be a stronger enforcement of them. According to StatsCan, out of the estimated 223,000 hate crimes that occurred in 2019, only 1% was addressed by the police. If law enforcement created specific units to pursue online hate, more resources can be dedicated to the disciplinary aspect of this ongoing issue.
- We implore the government to gather, clean, and disseminate disaggregated data on all marginalized groups affected by online hate. This can be integrated into the already proposed annual reports in order to ensure transparency. This data can inform legislation and the regulatory framework created by the independent digital safety commissioner.

Thank you for your efforts to tackle online hate and terrorism through the online harms consultation. We are grateful for the opportunity to submit comments and constructively contribute to a safer Canada.

We look forward to working with you on policy proposals that will benefit all Canadians. We are happy to answer any question you may have and are available at (email address)

Kindest regards,

Christopher Thompson

heatighter

Executive Director | Directeur exécutif cthompson@fbcfcn.ca Pronouns: He/ Him | II Languages: English | Anglais FEDERATION OF BLACK FEDERATION DES CANADIANS CANADIENS NOIRS Website | Twitter | Facebook | Linkedin

# Submission to the federal government's consultation on its proposed approach to address harmful content online

International Civil Liberties Monitoring Group

25 September 2021

The International Civil Liberties Monitoring Group is a coalition of 45 civil society organizations from a range of backgrounds and sectors from across Canada, including leading faith-based, labour, human rights, refugee and migrant, and environmental groups. Established in 2002, our mandate is to ensure the protection of civil liberties in Canada in the context of anti-terrorism and national security laws and activities.

Over the past two decades, we have participated in various government consultations and parliamentary hearings, intervened in court cases, issued multiple reports and engaged in popular education related to anti-terrorism legislation and national security activities. Throughout, we have documented how many of Canada's anti-terrorism laws have inflicted deep damage on fundamental freedoms, including freedom of expression, assembly and movement, privacy rights, due process, and equality rights (arising from racial and political profiling). Much of this is related to issues around government surveillance and profiling, information sharing between agencies (domestic and international), the use of secret hearings and secret evidence, the development of secret lists and legal regimes, lack of rigorous review and transparency, complicity in rights abuses such as indefinite detention and torture, and the overall expansion and "mission creep" of national security and anti-terrorism laws leading to ever-growing powers and a heavy reliance on security as a solution to social problems.

Our interest in the consultation regarding the government's proposal to address online harms lies in several areas. As a coalition whose mandate is to protect civil liberties, we also recognize the need to address real threats of violence and believe it is important and urgent that action is taken to address hate-based violence, and support government efforts to do so. It is clear that in supporting various freedoms, including freedom of expression, it is not enough to simply protect against cernsorship, but to also address actions and environments that make in impossible for invidividuals and communities to fully exercise their rights. We hope that our submission helps to strengthen and support that crucial policy goal.

However, we see several worrisome and even troubling aspects to this current proposal that may in fact undermine the stated goals. These include:

- the further expansion of problematic definitions of terrorism and enforcement online, which have been shown to more often target many the very communities which the government proposes to support with this new regime.
- a questionable conflation of efforts to address wildly different harms which need very specific solutions

- a monitoring and removal process that threatens freedom of expression and privacy rights, and which will likely have severe and significant impacts on already marginalized communities
- new obligatory reporting rules to law enforcement and intelligence agencies
- new warrant powers for CSIS
- transparency and accountability requirements that require the addition of more robust policies

In analyzing this proposal, our focus will be primarily on the interaction with anti-terrorism laws, policies and activities, as well as how they overlap and raise concerns for other areas. However, we recognize that the concerns we raise may not be applicable to all forms of "online harm" – although concerns about impacts on civil liberties and procedural fairness would likely apply in a general way to other areas as well.

#### A. Concerns about the consultation itself

The proposal is meant to address five areas of harmful content:

- Child sexual exploitation content
- The non-consensual sharing of intimate images
- Content which incites violence
- Hateful content
- Terrorism content

In the discussion guide and other public statements, the government has emphasized the consultation process leading up to this proposal. However, in our discussion with other civil society stakeholders, including those who have been consulted on other aspects of the proposal as well as ICLMG coalition members, none reported being engaged in regards to the "terrorism content" aspects of the proposed legislation.

Further, as has been raised by others, the timing of the consultation has also rendered full participation difficult. While the government announced the consultation on July 29th, with a deadline of Sept. 25th, the election call resulted in the cancellation of all in-person/virtual stakeholder meetings, making it impossible to ask questions or clarify aspects of the proposal. This would have greatly benefited in helping to ensure that submissions are as accurate and constructive as possible.

The fact the consultation was held during an election also meant that resources and capacity to participate were limited. This includes that, given the issue was associated directly with party platforms and promises, any substantial public engagement during the election period would have triggered the need to register as a third-party to the election and all the regulations it entails.

We are also concerned by the lack of supporting material explaining the necessity to implement a new regime targeting terrorism content online. We support the need to regulate online content

which incites violence, including content linked to terrorism. However, there are already multiple international efforts to do so that focus on the obligations of platforms overall. It is unclear from the consultation documents what the scope of the problem is in Canada, whether or not other efforts are succeeding or failing, and what would be judged a successful outcome of the new regime. These are issues which may have become clear if the consultation process had not been limited due to the elections; either way, the online materials would have benefited from such materials.

This is why we have joined with others in asking that the government extend the consultation process and delay tabling this proposal as a bill in Parliament until after this consultation process has concluded.

### B. Inclusion and impact of "terrorism content"

### Conflation of issues

We share the concerns raised by others that attempts to regulate multiple forms of harm under one overarching regime raises questions of effectiveness and appropriateness.<sup>1</sup> As we will discuss later, there is a lack of detail in regard to how the regime may be adapted to address the various types of harms. While we recognize that there are policy rationales for including various harms under one regime, it gives rise to various concerns.

First, it pre-supposes that a common approach on unrelated harms will effectively address each harm. As others have also argued, we believe that a more specific approach is necessary in order to adequately address each harm. By including these five harms together in one proposal, it is difficult to ensure that each area is dealt with appropriately. What is effective for one area may be unnecessary, or even detrimental, to another.

Second, we are concerned by the potential for "policy laundering," that is, using one policy goal in order to substantiate another, unrelated goal. By including new powers to monitor and report terrorism-related content in a proposal that also includes addressing child sexual exploitation content and the non-consensual sharing of intimate images, for example, renders it more difficult to question aspects of the bill because to do so would weaken regulation in other areas. We have seen this before in regard to proposals regarding lawful access and encryption, for example. It is essential that, when addressing such important and sensitive policy areas, that we are able to address them one by one. This proposal renders this kind of nuanced discussion difficult, if not impossible, and raises the possibility that tools that would not be acceptable if the proposal was related to terrorism alone are more easily adopted. This issue could perhaps have been resolved with a more in-depth consultation process, but would have been better resolved by crafting a proposal that addressed the nuances of each harm separately.

<sup>&</sup>lt;sup>1</sup>See, <u>https://internetsociety.ca/submission-to-the-department-of-canadian-heritage-consultation-on-internet-harms/;</u> https://ablawg.ca/2021/09/13/the-federal-governments-proposal-to-address-online-harms-explanation-and-critique/; https://www.michaelgeist.ca/2021/08/law-bytes-podcast-episode-99/

### Definition of "terrorist content"

As mentioned above, we recognize the need to regulate content that incites violence, including content related to terrorism, in order to avoid real-world harms.

However, such efforts must be targeted, clearly defined and demonstrate necessity and proportionality. Research, including our own, has demonstrated that terrorism is an incredibly difficult term to define.

The definition itself of "terrorism" is subject to controversy. It is almost impossible to reach consensus on it precisely because to say that some crimes are terrorist acts and some not is to make a judgment about the motive behind a crime. And that judgment will necessarily depend on the social, racial, religious, political or historical perspective of the people making the judgment. Using motive in this manner, as an essential element in defining and identifying a crime, is foreign to criminal law, humanitarian law, and the law regarding crimes against humanity. While a hate motive may be an aggravating factor at sentencing in the traditional criminal law, motive neither establishes nor excuses a crime.<sup>2</sup>

It is, therefore, never possible to create a definition of "terrorism" that is not either overinclusive or under-inclusive. It can be over-inclusive in that it captures ordinary crimes, civil disobedience, or the justified use of force against oppressive governments and occupations. It can be under-inclusive in that it excludes serious crimes and attacks against civilians that ought logically to be included, but are not, on purely political grounds.<sup>3</sup>

For instance, the definition fails to distinguish between criminal terrorist entities and liberation movements or groups opposing tyranny, whose legitimacy can shift depending on the time period and the dominating political interests at stake. Under this definition, Nobel Prize recipients Nelson Mandela and Rigoberta Menchu would be considered terrorists. Members of the French resistance fighting against the Nazi occupation were branded as "terrorists" by the Vichy authorities. More recently, participants in the 2011 Arab Spring protest movements against Egyptian dictator Hosni Mubarak have also been accused of being members of a "terrorist group" and deemed inadmissible due to security concerns, without evidence that they did more than engage in their right to freedom of expression and assembly.<sup>4</sup>

The definition does capture violent white supremacist groups, but we have seen how it also captures Palestinian and Kashmiri groups – as well as charities like IRFAN, proscribed for donating medical equipment to the Gaza Strip – conflating groups originating under or responding to long-term military occupation, with white supremacists and neo-Nazis, all under the rubric of a broad and inconsistent concept of "terrorism."

<sup>&</sup>lt;sup>2</sup> Canadian Association of University Teachers (CAUT), "Submission to the House of Common, Subcommittee on public safety and national security, regarding the *Anti-Terrorism Act*," February 28, 2005, p.31. Compulsion and necessity can be a defence, but under rare circumstances.

<sup>&</sup>lt;sup>3</sup> Ibid.

<sup>&</sup>lt;sup>4</sup> Nicolas Keung, "Egyptian asylum seeker with rights breached faces deportation," *The Toronto Star*, 21 April 2021. Online: <u>https://www.thestar.com/news/canada/2021/04/21/egyptian-asylum-seeker-with-rights-breached-faces-deportation.html</u>

This is why there is no international consensus in multilateral forums for a workable definition of terrorism.<sup>5</sup>

Beyond the application of terrorism laws by the justice system, the targeted use of accusations of terrorism by bad actors to target political opponents and marginalized communities is also well-documented. For example, supporters of the non-violent Boycott, Divestment and Sanctions movement in support of Palestinian human rights have been accused of both supporting terrorism and engaging in anti-Semitism.<sup>6</sup> Similarly, Indigenous land defenders have been accused by political opponents of engaging in or supporting terrorism for simply exercising their territorial rights<sup>7</sup>. Black Lives Matters activists have similarly seen accusations lobbed at them, leading to removal of content and suspension of social media accounts.<sup>8</sup>

Other examples could include:

- Academic work and reports on Palestinian human rights have been labelled as anti-Semitic and supporting terrorism, and could be made inaccessible based on automatic moderation or complaints.
- Calls for non-violent civil disobedience in support of Indigenous rights have been labeled by some Canadian politicians and media outlets as "terrorism." Would such postings be made inaccessible based on automatic moderation or complaints?
- Groups engaged in conflict often paint one or the other as "terrorist," particularly when one is a non-state actor and the other is a state actor. How will a platform decide what should be included as "terrorist" content, especially given the global application of the proposed regime?

The proposed system would allow for vague definitions of terrorism to be weaponized against those very groups that proposed legislation aims to support.

This renders both the proposed content moderation and reporting processes open to political arbitrariness and potentially vulnerable to manipulation for specific political interests.

Determining whether or not something consists of "terrorist content" is therefore already incredibly difficult to ascertain, even within the justice system. Adapting the current criminal code definition of "terrorism" to a regulatory framework, as proposed, would almost certainly mean an expansion of what content would fall under the definition. Social media companies would then be asked to develop both an automatic moderation system to make terrorism content inaccessible on their platforms as soon as possible, as well as to have staff not specifically trained in terrorism law to adjudicate, in a very short time frame, and under threat of financial

<sup>&</sup>lt;sup>5</sup> See, for example, Wesley S. McCann & Nicholas Pimley, "Mixed Mandates: Issues Concerning Organizational and Statutory Definitions of Terrorism in the United States," *Terrorism and Political Violence* (2020) 32:4, 807-830, DOI: 10.1080/09546553.2017.1404457

<sup>&</sup>lt;sup>6</sup> https://www.aljazeera.com/opinions/2016/2/28/eanada-jumps-on-the-anti-bds-bandwagon

<sup>7</sup> https://www.etvnews.ca/politics/conservative-mp-questions-whether-rail-blockades-constitute-terrorism-1.4830220

<sup>8</sup> https://www.usatodav.com/story/news/2019/04/24/facebook-while-black-zucked-users-say-they-get-blocked-racism-discussion/2859593002/

penalty, what consists of terrorism content and what does not. The result will almost certainly be the over-moderation of content, impacting not just freedom of expression, but also targeting the views of those communities that the proposed sets out to protect.

To inject an essentially political concept like "terrorism" into a legal framework is to ensure that politics, not law, determines culpability. If we are truly interested in condemning and prosecuting these crimes, it must be the act, not the motive that is determinative.<sup>9</sup>

Content that incites violence, whether terrorist or otherwise, would seem to be clearer and more precise.

### C. Moderation & appeal process

Our concerns around the application of "terrorist content" are exacerbated by the proposed moderation obligations and associated appeals process being put forward, particularly in combination with the proposed monetary penalties.

The proposal suggests that moderation would be carried out in two distinct ways in order to render harmful content inaccessible to people in Canada: via automatic moderation and complaints-based moderation. Both of these approaches carry with them distinct concerns.

Before addressing the specifics, there is an overarching concern about placing the determination of harmful content in the hands of private entities. The "privatization" of the decisions regarding discourse and public speech raises very specific concerns. As explained by Cynthia Khoo in "Deplatforming Misogyny," these kinds of questions should generally be considered by public institutions, and not private entities, particularly given that companies motivated by profit should not be relied upon to protect or advance issues of human rights or public good.<sup>10</sup>

To protect against this, we would argue that any policy proposal must include clear, restricted definitions of the content in question and strict reporting and enforcement rules, which we do not feel this proposal adequately contains in relations to terrorism content (and arguably other forms of content as well).

### Automatic moderation

The proposal would oblige included platforms to "take all reasonable measures, which can include the use of automated systems, to identify harmful content that is communicated on its OCS and that is accessible to persons in Canada, and to make that harmful content inaccessible to persons in Canada." It is likely that such automated systems would be powered by algorithms developed by platforms or third parties to identify and render inaccessible the targeted content.

<sup>&</sup>lt;sup>9</sup> Canadian Association of University Teachers, *supra* note 2, at 32.

<sup>10</sup> https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

This obligation goes much further than other comparable harmful content moderation regimes, including those in Germany, France and the UK, which purposefully do not include automated moderation of all content. While this is partially because of the restriction on doing so in the EU's e-Commerce Directive, it is primarily in recognition that such automated moderation of all content violates fundamental aspects of free expression by surveilling and monitoring all content for violations.<sup>11</sup> While the proposed system has been defended as being based on systems adopted in like-minded, rule of law countries, the fact that this proposal goes further than what has been accepted in those jurisdictions is often excluded from the conversation.

This filtering of content as it is published also raises a practical question: it would require that all content accessible by Canadians - and therefore all content published on, for example, Facebook - to undergo moderation. This would mean that content in a variety of languages and political and social contexts would need to be evaluated based on the Canadian government's definition of terrorism (and other harms). Therefore, any individual in the world posting to Facebook could be impacted by Canada's regulatory scheme. This could implicate large amounts of resources, and would possibly limit access of people in Canada to important and relevant content that, due to cultural or linguistic differences, would be automatically made inaccessible. As will be discussed later, it also raises questions about access and fairness in any appeals process.

Filtering by algorithm also raises concerns about the effectiveness and bias. As we have seen in multiple other contexts, reliance on algorithms to identify harmful language or content has led to disproportionate impacts on BIPOC, women and gender-diverse people.<sup>12</sup> There is no reason to expect a different result in the context of the proposed framework. In fact, we may expect even greater difficulty, as problems with algorithmic monitoring have been identified in more straightforward situations and clear definitions than that of "terrorist content."

While there are provisions in the proposal that such automatic moderation must "not result in differential treatment of any group based on a prohibited ground of discrimination within the meaning of the <u>Canadian Human Rights Act</u>," it is not clear that there would be proactive inspection of such algorithms (for example, via an initial review by the proposed Digital Safety Commission). It is also unclear to what degree or under what circumstances a member of the public could make a complaint if they believe that algorithms, overall, are resulting in "differential treatment of any group based on a prohibited ground of discrimination," particularly in the context of over-moderation which we imagine will be more difficult to monitor than, for example, under-moderation.

Finally, issues with an algorithm could conceivably be based on a characteristic other than a "prohibited ground for discrimination." For example, there could be unintended consequences of media or academic content not created by a member of a protected group being overly-moderated, as well as content from

<sup>&</sup>lt;sup>11</sup> https://www.eff.org/deeplinks/2021/07/uks-draft-online-safety-bill-raises-serious-concerns-around-freedomexpression; <u>https://www.counterextremism.com/sites/default/files/CEP-</u>

CEPS\_Germany%27s%20NetzDG\_020119.pdf

<sup>12</sup> See notes 6, 7, 8 & 10

Our understanding is that individuals whose content is made inaccessible by automatic moderation will be informed of this fact, including what steps can be taken to appeal the decision to make their content inaccessible.

### Complaint-based moderation

The proposed framework would allow for a new reporting system for people accessing a platform in Canada in order to signal harmful content, including terrorism content, to the platform in order to render it inaccessible. The platform would be required to act within 24 hours, informing the complainant whether they are taking action on the piece of content flagged and what action that is. If the piece of content is deemed harmful and is rendered inaccessible, the individual who posted the content would also be contacted. In both instances, the individual would be informed of the process for appealing the platform's decision.

This system is more widely used among jurisdictions similar to Canada's, including the UK and Germany. However, it has also met considerable opposition in those countries, and was even deemed largely unconstitutional in France.<sup>13</sup>

Concerns also exist around the short time period in which platforms must render a decision. It is clear that some forms of harmful content are readily identifiable as illegal, and would not be impacted by a mandatory 24-hour response time. However, large amounts of content including in regard to "terrorist content" will likely fall in a grey area of lawfulness or harmfulness, requiring examination of context or seeking out further information. To expect a decision within 24 hours, under penalty of non-compliance, would likely force a "render inaccessible first, ask questions later" approach. While the proposal makes explicit mention of setting different time periods by regulation (including shorter time periods), it positions 24 hours as the standard by which to decide all moderation decisions; it will be necessary to justify going forward why there should be longer time frames, rather than needing to justify a short time frame such as 24 hours. For example, in Germany, for grey area content, platforms have up to a week to make a moderation decision, and are able to request a further extension if necessary.<sup>14</sup> If this is the ultimate goal for the Canadian system, presenting these options clearly would have ensured a more comprehensive consultation and understanding of the moderation process.

Finally, while reports in Germany ostensibly point to fears of over-moderation of content having not played out, others have pointed out that a lack of clear and uniform reporting from platforms has made it difficult to ascertain the true impact (either positive or negative) of the system.<sup>15</sup> Once again, it is also important to bear in mind that this comparison is with a system based only on report-driven moderation, not automatic moderation as considered in the Canadian proposal.

<sup>13</sup> https://www.politico.eu/article/french-constitutional-court-strikes-down-most-of-hate-speech-law/

<sup>14</sup> https://www.ivir.nl/publicaties/download/NetzDG Tworek Leerssen April 2019.pdf

<sup>15</sup> https://policyreview.info/pdf/policyreview-2019-2-1398.pdf

### Appeal process

The proposal would allow an individual who disagrees with either the decision to leave a piece of content accessible, or to make it inaccessible, they would be able to appeal it to the platform (which, under the new framework, would be obliged to create an appeal process). Our understanding is that this is true whether the content is removed based on automatic moderation or through a user report; however, this must be further clarified.

If the individual is not satisfied with the platform's decision of their appeal, and has exhausted all avenues for appeal with the platform, they may appeal it to the newly proposed Digital Recourse Council of Canada (the Council). In the case of a complaint about content **not** being made inaccessible, and the Council rules that the platform erred, the Council can **order** the platform to make the content inaccessible. In the case of a complaint about content that **was** made inaccessible (asking that it should be restored), if the Council finds the platform erred, it can only **recommend** that the content be restored, but the platform has the final say based on its own community guidelines. This is clearly problematic, as it reduces the ability of individuals whose content has been removed to seek adequate recourse.

Also missing from the appeal process is clarity around timelines and accessibility. For example, a film festival specializing in Palestinian film is accused, unjustly, of programming content that supports terrorism. The festival's online event postings are either made inaccessible because of an algorithm or because of bad-faith reporting. The content is made inaccessible because of error in the algorithm or the need to adjudicate within 24 hours. the film festival appeals, and is eventually proven correct. The platform renders the content accessible, but the weeks-long process results in the content becoming no longer relevant, harming the festival and possible attendees. Arguably, the pursuit of reducing online harms is more important than access to a film festival; however, the impact is felt most strongly on a community that should ostensibly be protected by the new system rather than penalized.

Similar scenarios are possible when considering protests in support of Indigenous rights, given that Instagram has already removed content related to Missing and Murdered Indigenous Women and Girls, or acts in support of Black Lives Matters, which has also seen their content more heavily censored on social media platforms.<sup>16</sup>

While the appeal process is one of the more positive portions of this proposal, there are several outstanding concerns, particularly in relation to other aspects of the proposal. For example, the regime is global in scope, meaning that content posted from anywhere in the world is implicated, so long as it is accessible in Canada. It is likely, then, that individuals not in Canada will see their content removed and therefore need to engage in the Canadian appeal process. This is particularly true for automated moderation, since it can be assumed that most people in Canada will be engaging with content that is in a language they comprehend, shared in networks of their contacts, or referred to them by the platform itself.

<sup>&</sup>lt;sup>16</sup> See note 12

It is unclear whether an individual who is not in Canada will be familiar enough with the Canadian appeal process to engage with it, or be able to go through the process in one of Canada's major languages (platforms may specialize in providing service in a broad range of languages, but the Digital Recourse Council may not). They may also simply not care whether their content is available to people in Canada. The result could be that content that should otherwise be accessible to people in Canada would remain inaccessible. This would be a problem for content overall, but is even more important when such information may be necessary for research, journalistic or other purposes. For example, foreign language posts about a conflict in another region of the world are made inaccessible without cause due to over-breadth of automated moderation. Because the primary audience is not Canada, and because they do not speak a language commonly used in Canada, they decide not to appeal. Canadian audiences on social media would remain unaware of what content they do not have access to. This may seem far-fetched, but it could be possible that access to important and relevant information related to the Rohingya genocide, or the Arab Spring could have been blocked to Canadians.

### Monetary penalties

If a platform does not comply with their obligations, they face significant monetary penalties, ranging from \$10 million or 3% of income (whichever is higher), and \$25million or 5% of income in cases of non-compliance with sanctions. While financial penalties on their own are not necessarily problematic, in conjunction with short take down windows, they could provide yet another incentive for platforms to remove content in order to remain compliant. While in theory, sanctions could also be brought due to over-moderation it is likely that this would be much rarer than sanctions for lack of moderation.

### D. Information sharing with law enforcement and intelligence agencies

The framework proposes two options for sharing information with law enforcement and national security agencies. The first would "require that a [platform] notify the RCMP in circumstances where the [platform] has reasonable grounds to suspect that content falling within the five (5) categories of regulated harmful content reflects an imminent risk of serious harm to any person or to property."

The other is that a platform "must report prescribed information in respect of prescribed criminal offences falling within the five (5) categories of regulated harmful content to prescribed law enforcement officers or agencies, as may be prescribed through regulations established by the Governor in Council."

Both proposals would create new obligations to automatically report content to law enforcement and intelligence agencies, raising questions about the dangers of proactive reporting requirements, especially in light of "automatic moderation."

While the first appears more restrictive, requiring platforms to determine what constitutes "reasonable grounds to suspect" imminent risk of serious harm would likely result in overnotification. An automated system would also see such content shared with the RCMP without review, possibly sharing information that, after further appeal, is not considered as presenting "imminent risk of serious harm. It is also unclear why, if the goal is to oblige platforms to notify the RCMP in cases of imminent risk of serious harm, why that would be restricted only to risks that fall under the five categories. This is not an argument for expanding reporting obligations, but an example of how this approach fails to address the issue at hand.

The second proposal is the more troubling of the two. It creates an open-ended system of information sharing with many more law enforcement and intelligence agencies. In fact, the second proposal explicitly contemplates that any content related to terrorism or incitement to violence be shared immediately with CSIS.

Both scenarios also require the platforms to not disclose either notifications or reports "if the disclosure could prejudice a criminal investigation, whether or not a criminal investigation has begun" or "if the disclosure could be injurious to national security." This could mean that an individual would see their online content reported to law enforcement or national security agencies and never be informed, including if a criminal investigation never begins or on the incredibly broad grounds of "injurious to national security."

There is an attempt to mitigate this issue by including the following section:

Retention period and use:

32. The Act should provide the Governor in Council with the authority to make regulations with respect to the use and subsequent disclosures of information provided to (a) the RCMP or (b) law enforcement and CSIS under part [E], **depending on the privacy interests engaged by that information.** [emphasis added]

Here, though, the relevant phrase is "depending on the privacy interests engaged by that information." It is likely that content posted on social media platforms would have a low-level privacy interest, although this is currently disputed by privacy advocates given that content posted on social media platforms, while accessible, may still retain some expectation of privacy from government agencies. Further, since this system would be applicable to non-Canadians outside of Canada, they would not be granted the same privacy interests as Canadians or people in Canada.

While platforms are also obliged to ensure that the reporting to law enforcement / security agencies does not result in "differential treatment of any group based on a prohibited ground of discrimination within the meaning of the <u>Canadian Human Rights Act</u> and in accordance with regulations," we have seen how agencies defend surveillance and profiling of specific communities on the basis of national security in order to avoid accusations of "differential treatment."

Finally, the framework proposes that platforms who report to CSIS and the RCMP or other agencies in good faith pursuant to the act would be immune to civil or criminal proceedings. So, for example, if a platform's auto-reporting system accidentally sends information that results in

the violation of an individual's rights, including surveillance or possible detention, they cannot hold the platform accountable for that action.

Again, all the issues above are exacerbated by the underlying problems in identifying terrorist content highlighted earlier.

The result is that social media platforms would essentially be recruited and turned into extensions of the surveillance tools already at the disposal of Canada's law enforcement and intelligence agencies.

### E. New CSIS warrant

The proposal also makes the extraordinary argument that CSIS be granted a new form of warrant. Arguing that CSIS is currently limited to one kind of warrant that takes several months to process, the proposal suggests a new "simplified" process for seeking out a judicial authorization for obtaining identifying information (basic subscriber information, or BSI) in order to aid with the investigation of online harms.

While it may be true that the current judicial authorization process is not adequate for CSIS to assist in the investigation of online harms, this is a secondary issue. The first is whether CSIS should be recruited into this form of investigation in the first place. While action must be taken to address threats of white supremacist and hate-based violence, this should not be used to justify the further granting of police-like powers to an intelligence agency that operates in secret. We have already seen CSIS granted threat-disruption powers that mimic those of the police. This new form of warrant would further entrench the idea of CSIS investigating criminal activity akin to law enforcement, well beyond its role as an intelligence agency.

If there is a problem with CSIS not being able to carry out its intelligence work regarding threats to national security, it should be addressed in a stand-alone bill and justified on those grounds.

Finally, any new warrant power would not be limited to investigating online harms, but could be harnessed in other areas of CSIS' work as well. At a time where there are serious questions before the court about CSIS' breach of its duty of candour in warrant applications, it is concerning that the government would be proposing to create a new, simplified and flexible process for obtaining judicial authorization to collect information about individuals.

### F. Transparency and accountability

As mentioned above, there are certain requirements placed upon the platforms to report to the Data Commissioner annually. This is an important and positive part of the proposal, especially in terms of integrating concerns that have been raised in other jurisdictions about problems with reporting. However, it is crucial that this reporting be strengthened in several ways.:

- 1. Other jurisdictions require platforms to publish publicly available transparency reports on a regular interval (for example, every six months in Germany). The Canadian proposal should include similar requirements.
- 2. While the Digital Safety Commissioner and Recourse Council are required to make extensive reports to the Minister, there are no provisions that such reports will be tabled in Parliament. It is crucial that such reports be made public.
- 3. Given the role of the RCMP and/or CSIS, they should be required to report separately to the Minister of Public Safety, to be tabled in parliament. And these reports should be proactively shared with the Privacy Commissioner, CCRC and NSIRA.

### Conclusion

Our coalition has not taken a position on the need for new regulations related to online harms. Indeed, in much of our recent work we have taken the position that more needs to be done to protect various communities, including BIPOC, women and gender diverse people, from growing violence and threats from white supremacist, far right or misogynist organizations. The lack of action in this area by social media platforms has been well documented by groups including LEAF and Amnesty International Canada<sup>17</sup>.

However, over the past two decades, we have seen the impact that expanding national security and anti-terrorism laws have had on the rights of people in Canada, and internationally. This is particularly true for Muslim, Arab, Indigenous and other racialized communities and their allies who have faced profiling, disproportionate policing and other human rights abuses. Moreover, growing surveillance predicated on countering terrorism has overarching impacts on privacy, freedom of expression, freedom of association and freedom of movement.

We believe that in order to achieve the stated goals of the government's proposal - to counter real world harms faced by protected classes of individuals as defined in the Canadian Human Rights Act - that it must be reviewed with the issues we lay out above in mind, particularly in regard to the inclusion of "terrorist content" and the involvement of law enforcement and national security agencies in any new regime.

<sup>&</sup>lt;sup>17</sup> https://www.annesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-1/; https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

ht Leo and Toromba & FORDProvident Disconnent verheinent zursunnt inthe Aresis Reativements (44)

FASKEN

Fasken Martineau DuMoulin LLP Barristers and Solicitors Patent and Trade-mark Agents 55 Metcalfe Street, Suite 1300 Otrawa, Ontario K1P 6L5 Ganada T +1 613 236 3882 +1 877 609 5685 F +1 613 230 6423

fasken.com

Jay Kerr-Wilson Direct +1 613 696 6884 jkerrwilson@fasken.com

September 25, 2021

By Email Pch.icn-dci.pch@canada.ca

Re: TSPs' Submission to the Government's proposed approach to address harmful content online

### Introduction

We are pleased to provide these comments on behalf of Bell Canada, Rogers Communications, Shaw Communications, TELUS Communications, Cogeco Communications, and Quebecor Media (collectively the "Telecommunications Service Providers" or "TSPs"). We use the terms "Telecommunications Service Providers" or "TSPs" to refer to all intermediaries that provide residential and commercial subscribers with access to the internet via wireline or wireless network. Combined, these TSPs provide internet access and other telecommunications services to the vast majority of Canadian households and businesses. The TSPs appreciate this opportunity to present their views on the Government's proposed approach to address harmful content online.

As a preliminary matter, the TSPs want to express concern with the process by which these comments were sought – specifically, the lack of clarity with respect to the deadline for submissions. The deadline was not posted on the consultation page<sup>1</sup> nor was it contained in either of the linked Discussion Document or Technical Paper. Accordingly, the comments below represent preliminary feedback of the TSPs on the proposed approach and the TSPs reserve the right to make further submissions in connection with this consultation. More broadly, the TSPs strongly recommend that the consultation be extended – not only because of the procedural shortcomings with the consultation notices as posted, but also because the consultation period was excessively short given the importance of the subject matter, the complexity of the proposals, and the consultation ran concurrently with a federal election period during which public attention was largely focussed on a wide range of political issues.

Robust and reliable networks built and maintained by the TSPs are essential to Canadians' social and political engagement, access to entertainment, educational, and cultural offerings, and ability to benefit from economic opportunities. The TSPs have and will continue to invest significantly in their infrastructure in order to provide the level of service required by Canadians. The speed, reliability and capacity of Canada's communications networks are continuously being improved.

<sup>&</sup>lt;sup>1</sup> https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.htm

# FASKEN

The fundamental function of the service that TSPs provide is the same as it has always been—providing passive connectivity service to Canadian homes and businesses. TSPs should not face any new liability for providing an increasingly essential service over complex networks that have been built and upgraded for decades.

The TSPs support the Government's goal of supporting safe, inclusive, and open online environments. They recognize that in addition to the immense cultural, social, and economic benefits delivered by Canada's technologically-advanced communications networks, some online platforms are used by some users to spread hate speech, terrorist propaganda and other harmful or illegal content, including the exploitation of children.

Canada's legal framework should address the problem of online harmful content by adopting regulatory and enforcement measures that are technically feasible, effectively target the source of the harmful content, and respect constitutional requirements for due process and judicial oversight.

### Importance of protecting investment in networks

The TSPs strongly support the Government's proposed approach that would explicitly exempt from the scope of the legislation telecommunications service providers such as the TSPs, private communications and certain technical operators.

In its consultation guide, the Government recognizes that "social media platforms and other online communications services play a vital and important role in Canada's society and economy". TSPs provide the telecommunications networks upon which these emerging new communications technologies and platforms are built. Access to next generation mobile services and applications, including Internet of Things devices and advancements, would not be possible without robust infrastructure built by TSPs. The Internet of Things describes a network of connected devices beyond computers, smartphones, and tablets.<sup>2</sup> This network is transforming supply chains and giving consumers access to a wide variety of personalized services. Network investments will and must continue to grow going forward to meet Canadian demand for advanced Internet-based products and services.

5G in particular promises to be one of the most transformative communications technologies since wireless services were first introduced. Immense improvements in bandwidth, latency, connection density and reliability as a result of 5G network transformation will be a necessary precursor to the proliferation of new use cases for the newest applications and devices which facilitate data-intense Internet usage. If Canadian companies and innovators are going to be leaders in developing the next generation of intelligent applications that will drive innovation in Industry 4.0 and produce significant economic, employment, environmental, and other benefits for Canadians, world-leading 5G networks will be an absolute necessity.

<sup>&</sup>lt;sup>2</sup> A Consultation on a Modern Copyright Framework for Artificial Intelligence and the Internet of Things, Innovation, Science and Economic Development of Canada (2021), quoting "State of the IoT 2020: 12 billion IoT Connections, surpassing non IoT for the first time".

### FASKEN

Building the robust 5G networks that will fuel these advances will require staggering financial investment by Canada's facilities-based TSPs. The Canadian Wireless Telecommunications Association estimates that Canadian carriers will need to invest over \$26 billion to deploy the physical network infrastructure associated with 5G networks in Canada. In addition, Canadian carriers have already started to spend billions more to acquire the right to use key 5G mobile spectrum over that same time period. Canada's recent auction of 3500 MHz spectrum (an essential mid-band spectrum for 5G networks) generated a record \$8.9 billion in revenue for the Government of Canada, and there are many other high-band frequencies that will be auctioned off in the next two years.

Given the high stakes associated with the race to developing 5G networks, it is essential that the modernized Canadian legal framework for addressing harmful online content does not create additional obligations or liability for carriers, which could impact internet costs and disincentivize Canadian TSPs from making the investments in 5G networks required to harness the next wave of innovation in Canada.

# Measures need to be consistent with Canadian law, technically feasible, rely on judicial oversight, and provide for cost recovery

TSPs do not possess the considerable expertise or human resources required to proactively monitor their subscribers' online activities for potential harmful content. It would be an affront to the fundamental concept of an open internet and basic civil liberties to require TSPs to engage in this kind of proactive monitoring of Canadians' online activities and would compromise Canadians' confidence in TSPs as neutral and passive network service providers. Such an obligation may also contradict the privacy policies of many TSPs, some of whom make positive assertions to their subscribers that they do not monitor their online activity. Without compelling and well-defined exigent circumstances TSPs should only be required to disable access to online content in response to a judicial order. TSPs are already subject to the Mandatory Reporting Act which applies to the discovery of exploitative images of children, but incidents of TSPs encountering this type of material are exceedingly rare.

Similarly, the Government should not require ISPs to provide basic subscriber information or transmission data without judicial authorization. It is not clear that eliminating the need for judicial authorization would be justified when weighed against the need to protect the privacy interests and constitutional rights of Canadians. Any concerns about undue delays are better addressed by implementing expedited processes for law enforcement agencies to obtain judicial orders. Such processes could include the appointment of specialized judicial officials available around the clock to consider applications and issue orders.

If TSPs are required to provide subscriber information and transmission data without judicial authorization (a requirement to which, as noted above, TSPs are opposed), it should only be done with extreme caution in well-defined exigent circumstances, and TSPs should be provided with comprehensive safe harbour protections against any claims arising from their compliance with

# FASKEN

these obligations. Any requirement to provide subscriber information and transmission data should apply only to the extent the TSP is able to provide the data. There can be technical issues that prevent a TSP from accurately identifying a subscriber, such as the use of virtual private networks (VPNs) or IP spoofing.

Any approach to regulating harmful online content must be consistent with TSPs' technical capabilities and limitations. TSPs generally lack the technical ability to disable access to information within the platform of an Online Communication Service Provider (OCSP), such as the specific posts or comments made by the users of these platforms. This type of precise intervention should only be undertaken by the OCSP themselves. While TSPs can, and do, disable access to harmful and illegal content in response to Court orders, these orders target specific domain names or IP addresses. This has the effect of disabling access to the entire platform or site that uses that name or IP address and would affect any lawful content hosted on the platform or server in addition to the illegal content that is the subject of the intervention.

Given the risks associated with "overblocking" lawful online content, and the potential damage that could be caused to legitimate businesses if their e-commerce platforms were taken down as collateral damage in response to a blocking order, TSPs must be legally indemnified against civil damages and other consequences in the event that complying with any legal requirement, including but not limited to a Court order, has such an effect on legitimate content. It is also important that any judicial blocking order apply equally to all internet service providers (ISPs) in order to avoid any competitive imbalance between any two ISPs and ensure that any measures apply equally to all internet users in Canada and avoid creating safe havens for illegal and harmful content online.

TSPs must also be able to recover their reasonable costs of complying with judicial orders to disclose subscriber information and transmission data, disable access to online content or facilitate other types of lawful interception of telecommunications. The costs of TSPs' compliance with judicial orders or any other legal requirements in connection with addressing harmful online content should not be borne by TSPs, as such costs could have negative impacts on TSPs' customers as well as TSPs' resources available to build, upgrade and maintain network infrastructure.

### Conclusion

The TSPs appreciate this opportunity to comment on the Consultation and look forward to continuing discussion on these issues.

Document communiqué en vient de la La sur l'acole à l'information Document milésoit pursuaré lo lite Access la misemation Act

# FASKEN

Yours truly,

FASKEN MARTINEAU DUMOULIN LLP

Verr-Wil

Jay Kerr-Wilson



Dissummit commonique en versioni la Lin aux canaga à l'information Distancent mécacett donation fit discusses la matematica en



# Submission in relation to the consultation on addressing harmful content online

September 25, 2021

Cara Zwibel, Director, Fundamental Freedoms Program

Canadian Civil Liberties Association 90 Eglinton Ave. E., Suite 900 Toronto, ON M4P 2Y3 Phone: 416-363-0321 www.ccla.org

### 1. Introduction

The Canadian Civil Liberties Association ("CCLA") is an independent, national, nongovernmental organization that was founded in 1964 with a mandate to defend and foster the civil liberties, human rights, and democratic freedoms of all people across Canada. Our work encompasses advocacy, research, and litigation related to the criminal justice system, equality rights, privacy rights, and fundamental constitutional freedoms.

We recognize the public pressure on governments to "do something" about the Wild West of online content. With this proposal, however, the Heritage Ministry is addressing areas far outside its core expertise; it ought not to be stewarding legislation that so impacts Canada's foreign affairs, anti-terrorism and criminal laws. Consulting with other Ministries and other jurisdictions and stakeholders will not suffice, any more than one would want Foreign Affairs to regulate the radio broadcast industry. This may explain the proposal's over breadth.

The CCLA has several concerns about the government's proposed approach to "online harms" as well as concerns about the way this consultation is being undertaken. Considering the timing of this consultation process (discussed briefly below), our submissions on the substantive concerns about the proposal are set out in brief and are not exhaustive. This should not be misinterpreted to suggest that CCLA has little to say about the proposal. To the contrary, we believe a policy issue of this level of importance, and a proposal with such novel elements, must be subject to more rigorous scrutiny. We welcome the chance to be part of more meaningful discussions in the future; we will strongly resist attempts to push through legislation on this issue in the absence of truly inclusive and substantive consultations with Canadians.

The proposal is a radical policy change, in our view. It is excessive in scope, effect and purpose. CCLA's substantive concerns about the proposal include the following:

- The scope of the proposal problematically attempts to deal with a variety of different "online harms" and not solely unlawful content. This amounts to significant regulation of the ways in which Canadians communicate. The proposal also fails to appreciate how different the content categories are and the possibility that they may need to be addressed using different policy tools.
- 2) The proposal merges communications policy/regulation with public safety, national security and law enforcement concerns in a way that is quite troubling. Mandatory reporting by online communications service providers (OCSPs), as tentatively defined in the proposal, give rise to significant questions about the use of artificial intelligence and over-reporting, as well as state surveillance and the role of large platforms in its facilitation. The law enforcement proposals would also leave a great deal of detail to be decided by regulation, leading to concerns about political interference and the absence of meaningful democratic debate.
- 3) The proposal includes 24-hour takedown requirements for platforms for a wide variety of content and fails to consider the significant risk to lawful expression posed by this requirement. There are few meaningful due process protections built into this scheme.

4) The proposal includes a power to seek website blocking orders. Although this is touted in this context as a means of making the internet safer, site blocking presents a real threat to an open and safe internet. Clear and meaningful safeguards are required if such a power is deemed necessary in extraordinary circumstances.

CCLA does welcome the proposal's inclusion of new transparency obligations for online communication service providers (OCSPs), although care should be taken to ensure that a push for transparency from platforms doesn't inadvertently impinge on user privacy by requiring platforms to collect more information from users in order to fulfill their statutorily-mandated reporting requirements.

With respect to process, we note that the government's proposal for addressing harmful content online was released on July 29, 2021 and the closing date for submissions is September 25, 2021. A federal election was called on August 15 and voters cast their ballots on September 20, 2021. Thus, throughout much of the consultation period, it was unclear whether the government that undertook it would be elected and form a government. As noted in an <u>open letter</u> to individuals in the Privy Council Office and to which CCLA was a signatory, guidance on the activities of government after Parliament is dissolved states that policy work should be limited to routine, non-controversial or urgent areas, or where there is agreement by opposition parties. The online harms policy question falls into none of these categories. It is a complex area that raises fundamental questions about communications in Canada, human rights, corporate social responsibility, and the role of the state in regulating and monitoring Canadians' expression.

This issue deserves careful consideration and meaningful engagement with Canadians. To ask civil society to provide feedback to a government proposal when it is unclear if that government will return to govern is insufficiently respectful of the time and efforts that civil society organizations expend on these kinds of consultations. It is also likely to diminish the breadth and depth of submissions the government receives. Further, the government's proposal in this case is very detailed and in fact asks very few questions of those interested in participating in the consultation process, suggesting that the government has largely already decided what it intends to do. We strongly believe that a much more robust consultation process should be undertaken as soon as possible.

### II. The Scope of "Online Harms"

Throughout the consultation documents and in messaging from the government, the focus of the proposal has been on tackling "online harms". This suggests that it targets content that is *harmful* but not necessarily *unlawful*. This is inappropriate. The focus of any legislative proposal should be on illegal content. Although the government's technical document notes that the content categories will use definitions that borrow from the *Criminal Code*, it also states that these categories will be adapted to the "regulatory context". It is not clear what exactly this language means, or how it will apply to the different types of content. The proposal also notes that there will be authority for the Governor in Council to, by regulation, define certain specific terms used in the definitions of harmful content. Thus the scope of the law, and the kinds of content it may capture, can be expanded without any meaningful democratic oversight. The expressive freedom guaranteed by the *Charter* dictates that lawful communications should not be the subject of

government restrictions, but the proposal could be used to restrict the so-called "lawful but awful" content online.

The government's proposal also groups together five quite different types of "harmful" content: child sexual exploitation content, terrorist content, content that incites violence, hate speech and the non-consensual sharing of intimate images. Not only are these content categories very different, but the types of harms to which they give rise also vary considerably. For example, while hate speech may constitute a criminal offence in some contexts (e.g. where the communication is willful and intended to promote hatred and where the hallmarks of hate identified by the Supreme Court are present), the acts that result in visual depictions of child sexual exploitation are themselves criminal in almost any circumstance and there are offences not only for creating and distributing this material, but also for accessing it. As a result, some of the categories of content will require a greater understanding of context to assess legality, while others will be more obvious and easier to identify either using automation or manual human review. The types of content have little in common with one another except that they may be communicated in the same type of online space, through OCSPs. Given these differences, it is questionable whether these diverse types of content should be addressed using identical policy tools.

### III. Public Safety and State Surveillance

The CCLA has significant concerns about the proposal's plans to leverage OCSPs as agents of law enforcement, creating mandatory reporting and preservation obligations that may expand over time and significantly impact the privacy rights of Canadians. The involvement of CSIS is of particular concern.

Further, while we appreciate that adequately addressing some of the harms identified in the proposal will require the assistance of law enforcement, the feasibility of mandatory reporting on this scale is far from evident. The sheer volume of content that some OCSPs would have to proactively review and potentially report suggests that the use of artificial intelligence is inevitable. It is likely that some content will be assessed and reported to law enforcement based exclusively on algorithms that will have a rate of false positives. The consequences to an individual of being flagged for police investigation are significant. The proposal contains no consideration of these consequences or the due process protections that might mitigate them.

The two options proposed in the government's technical document each have serious flaws. The first option is focused on reports where the OSCP has reasonable grounds to suspect there is an imminent risk of serious harm to any person or to property. However, the focus on imminent harm suggests that OCSPs are expected to proactively review and report content in real-time, something that is not feasible for the reasons outlined above. The second option requires OCSPs to report "prescribed information in respect of prescribed criminal offences falling within the five (5) categories of regulated harmful content to prescribed law enforcement officers or agencies, as may be prescribed." It is difficult to comment on a proposal that leaves so many details to regulation. The question of when online communications should be turned over to law enforcement officials is something that should be the subject of debate in Parliament.

### IV. Twenty-Four Hour Takedown

The government's proposal creates several new obligations on OCSPs including responding to individuals who flag content as falling within one of the prohibited categories within twenty-four hours of the flagging taking place. If the OCSP finds that the content does fall into one of the categories, it is to be made inaccessible to individuals in Canada within that twenty-four-hour period, although the Governor in Council may both extend that period or shorten it in respect of certain types of content.

The diverse types of content that the proposal targets each have their own unique characteristics and while some may be easy to identify, others will be much more difficult, particularly under severe time pressure and where the volume of content is large. Identifying *illegal* hate speech and terrorist content, for example, is not an easy task if one takes seriously the obligation to interpret these terms narrowly to avoid unreasonably restricting freedom of expression. Even judges who are trained in statutory interpretation and constitutional law may disagree about what falls on the right or wrong side of the line with respect to these types of content, yet the proposal imagines that OCSPs will be able to make these determinations for potentially huge volumes of content within 24 hours. There is no requirement in the proposal that these providers receive any training or have any background understanding of Canadian law. If OCSPs are going to be the "front line" when it comes to policing Canadians' communications online, it is important that they understand the proper scope of the law, and its constitutional limits.

Further, experience in other jurisdictions and the sheer scale of content on some OCSPs strongly suggests that content will be removed when there is any doubt about its legality, and not solely when its illegality is plain and obvious. Rather than erring on the side of caution, platforms have incentives to remove content quickly where judgments are difficult to make. It is worth noting that the <u>Canadian Commission on Democratic Expression</u> rejected the idea of 24-hour takedowns for content, except for the narrow category of content that presents an imminent threat to a person. CCLA believes this standard is more in keeping with Canada's commitments to freedom of expression and deals appropriately with the most egregious and potentially dangerous forms of online content. The government should eliminate the 24-hour takedown or to dramatically reduce the scope of content to which it applies.

### V. Website Blocking

The proposal seeks to establish a scheme to apply to a court for a website blocking order. Although the suggestion is that this would be used in exceptional circumstances for repeat offending conduct by OCSPs, it is worth emphasizing that website blocking is a truly extraordinary remedy when imposed by a state body. This tool will often be both inefficient and ineffective, resulting in a game of whack-a-mole as repeat offenders move to new online spaces to engage in the targeted conduct. There are also technical concerns about website blocking and how it will impact the online ecosystem as a whole.

### VI. Transparency Obligations

Finally, we welcome many of the proposals to increase the transparency required from OCSPs. This information is vitally important for any regulatory efforts and can help encourage responsible

corporate behaviour. However, many of the reporting requirements call for a significant amount of detail from service providers which may impact the information they, in turn, have to collect from their users. This is not a trivial concern. We already have significant experience and concerns about the way in which some platforms collect and utilize user information. When paired with the transparency obligations and the mandatory reports to law enforcement, user privacy is at significant risk from this proposal. The transparency obligations should be crafted in a way that does not have unintended consequences for user privacy.

### VII. Conclusion

As noted above, the CCLA is concerned about the substance of the government's proposal to address online harms, and about the manner in which the government has treated this issue and public consultation. Regulating the way in which Canadians communicate online – including the content that they may access from locations all around the globe – is a significant public policy project that merits broad participation and involvement from Canadians. Further, many countries look to Canada as a mature liberal democracy and may seek to emulate the tools developed for tackling online harms here. Twenty-four-hour takedown requirements and website blocking orders are dangerous tools anywhere, but may be of heightened concern in the hands of regimes that have a lesser commitment to democracy. Given the truly global nature of the internet, this is a concern that the government should take seriously.

This submission is brief given the inadequate time provided for consultation; we have highlighted some of our core concerns but have others that are not addressed herein. The government should not introduce legislation in this policy area until a more fulsome consultation process has taken place. We look forward to participating in that process.

### Subject: Joint submission re: Online harms legislation 25.09.2021

### (La version française suit)

To whom it may concern:

As organizations and individuals with expertise in anti-racism, we are profoundly concerned by the government's proposed "online harms" legislation – purporting to address "terrorist content," "content that incites violence," "hate speech," "non-consensual sharing of intimate images," and "child sexual exploitation content."<sup>1</sup>

While the proposal is billed as protecting marginalized groups from "hate, harassment, and violent rhetoric online," we fear that, as currently formulated, it risks exacerbating the existing, well-documented pattern of online speech policing and removal targeting Indigenous, Black, Palestinian, and other colonized and racialized communities.<sup>2</sup>

Particular aspects of concern regarding the proposed legislative framework from an anti-racism perspective include:

- Incentivization of over-removal produced by: the short timeline for required response after content being flagged (24 hours); the obligation for online communication service providers (OCSPs) to take proactive measures to identify harmful content, including through use of automated systems (repeatedly shown susceptible to amplifying existing biases<sup>3</sup>); vague definitions that will lead platforms to be over-inclusive in order to be "safe;" and significant financial penalties for non-compliance.
- 2) Conflation of very different types of online harms for example, "hateful" or "terrorist" content with "child sexual exploitation" or "non-consensual sharing of intimate images"<sup>4</sup> – under a single regulatory regime. This is particularly problematic given the existing deployment of categories of "hate speech" and

https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html#a3a4
 For example:

https://www.ctvnews.ca/sci-tech/complaints-flood-social-media-as-indigenous-stories-disappear-on-instagram-1.541 8147;

https://www.vox.com/recode/2019/8/15/20806384/social-media-hate-speech-bias-black-african-american-facebook-t witter https://7amleh.org/storage/The%20Attacks%20on%20Palestinian%20Digital%20Rights.pdf. <sup>3</sup> https://undoes.org/pdf?symbol=en/A/73/348

<sup>&</sup>lt;sup>4</sup> See e.g. https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3586056 and

https://www.leaf.ca/publication/deplatforming-misogyny/ that focus specifically on non-consensual sharing of intimate images and technology-facilitated gender-based violence.

"terrorist speech" to censor Black and Palestinian content online<sup>5</sup>; abetted, in the Palestinian case, by efforts to institutionalize the International Holocaust Remembrance Alliance definition of antisemitism, widely critiqued for conflating criticisms of Israeli policy with antisemitism.<sup>6</sup>

- 3) Increased information-sharing with law enforcement and security agencies regarding possibly harmful content. As law and technology scholar Michael Geist observes, this may "lead to the prospect of [artificial intelligence] identifying what it thinks is content caught by the law and generating a report to the RCMP"<sup>7</sup> – likely intensifying the current state of over-policing and -surveillance of colonized and racialized communities.<sup>8</sup>
- 4) Sweeping search powers for "inspectors" to verify compliance with the legislation, secret hearings, and new information-gathering powers for CSIS allocating further police-like capacities to CSIS.
- 5) Absence of adequate transparency, accountability, and redress measures with no clear mechanisms for publicly assessing whether Internet companies are fulfilling their obligation to prevent discriminatory treatment in content removal and reporting to law enforcement and CSIS; the protection of companies from criminal and civil liability for notifications to law enforcement and CSIS made in "good faith"; and no requirement to restore content found to be wrongfully removed, deferring to Internet companies' own community standards. As three UN Special Rapporteurs recently noted, "such terms of service or community standards do not reference human rights and related responsibilities, thereby creating the possibility of an 'escape route' from human rights oversight."<sup>9</sup>

According to Daphne Keller, Director of the Program on Platform Regulation at Stanford's Cyber Policy Center, Canada's proposal is **"like a list of the worst ideas around the world** – the ones human rights groups ... have been fighting in the EU, India, Australia, Singapore, Indonesia, and elsewhere."<sup>10</sup>

<sup>&</sup>lt;sup>5</sup> https://homes.cs.washington.edu/~msap/pdfs/sap2019risk.pdf;

https://www.usatoday.com/story/news/2019/04/24/facebook-while-black-zucked-users-say-they-get-blocked-racismdiscussion/2859593002/;

https://www.aclu.org/news/free-speech/time-and-again-social-media-giants-get-content-moderation-wrong-silencing -speech-about-al-aqsa-mosque-is-just-the-latest-example/

<sup>&</sup>lt;sup>6</sup> https://blogs.timesofisrael.com/whos-against-adopting-the-ihra-antisemitism-definition/;

https://www.ijvcanada.org/tackling-online-hate-letter/

<sup>&</sup>lt;sup>7</sup> https://www.michaelgeist.ca/2021/07/onlineharnisnonconsult/.

<sup>8</sup> https://fernwoodpublishing\_ca/book/policing-black-lives;

https://books.google.ca/books/about/Policing\_Indigenous\_Movements.html?id=NtoOtAEACAAJ&redir\_esc=y

<sup>&</sup>lt;sup>9</sup> https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gld=24234

<sup>10</sup> https://twitter.com/daphnehk/status/1421120217585831938

Our concerns are compounded by troubling deficiencies in the government's ongoing consultation process organized to validate the proposed legislation. Expert perspectives on addressing harmful speech online while protecting civil liberties have reportedly been disregarded.<sup>11</sup> Planned consultation meetings with community representatives have been cancelled due to the election, yet the deadline for the consultation period remains as previously advertised, September 25 – just five days after the election.

Given the serious risks posed by the proposed "online harms" legislation – including to the very communities it is represented as protecting – we call for the government to suspend any implementation, until a full, fair, open, and responsive consultation with anti-racism, human rights, and civil liberties experts has taken place, and the problems and pitfalls identified have been rectified.

111

### Madame, Monsieur :

En tant qu'organisations et personnes ayant une expertise en matière d'anti-racisme, nous sommes extrêmement préoccupées par le projet de loi du gouvernement qui se veut une solution aux «contenus préjudiciables en ligne», soit les contenus «terroristes», ceux «incitant à la violence», ceux concernant le «partage non consensuel d'images intimes» et «l'exploitation sexuelle des enfants.» [1]

Bien que l'intention derrière le projet de loi est de protéger les groupes marginalisés contre la «haine, le harcèlement et la rhétorique violente en ligne», nous craignons que, telle que présentée, la législation proposée risque plutôt d'exacerber la tendance bien documentée de cibler et supprimer le contenu en ligne au sujet d'enjeux soulevés par les communautés autochtones, palestinien.nes, noires et autres communautés racisées et colonisées. [2]

D'un point de vue antiraciste, le cadre législatif proposé soulève les préoccupations suivantes:

1) **L'incitation à la suppression excessive de contenu, en raison** : du délai très court (24 heures) pour éliminer un contenu suspect; de l'obligation pour les fournisseurs de services de communication en ligne d'être proactif dans le repérage de contenus préjudiciables, y compris à travers le recours à des systèmes automatisés (alors qu'il a été démontré qu'ils amplifient les préjugés existants [3]); des définitions vagues qui pousseront les plateformes

<sup>11</sup> 

https://www.michaelgeist.ca/podcast/episode-99-they-just-seemed-not-to-listen-to-any-of-us-cynthia-khoo-on-the-ca nadian-governments-online-harms-consultation/?utm\_source=rss&utm\_medium=rss&utm\_campaign=episode-99-th ey-just-seemed-not-to-listen-to-any-of-us-cynthia-khoo-on-the-canadian-governments-online-harms-consultation

à cibler plus largement par «prudence»; et des pénalités financières importantes en cas de non conformité.

2) L'amalgame, sous un seul régime réglementaire, de contenus préjudiciables disparates – par exemple, le contenu «haineux» ou «terroriste» avec le «partage non consensuel d'images intimes» ou «l'exploitation sexuelle des enfants» [4]. Cela est particulièrement problématique compte tenu que les notions de «discours haineux» et «discours terroriste» sont déjà utilisées pour censurer le contenu en ligne lié à des enjeux soulevés par les communautés noire et palestinienne [5]; un problème exacerbé, dans le cas des Palestinien.nes, par les efforts d'institutionnaliser la définition de l'antisémitisme de l'Alliance internationale pour la mémoire de l'Holocauste (IHRA), largement critiquée pour son amalgame de la critique des politiques israéliennes avec l'antisémitisme. [6]

3) Le partage accru d'information avec les agences de renseignement et les forces policières concernant des contenus potentiellement préjudiciables. Comme le souligne Michael Geist, spécialiste en droit et en technologie, ceci pourrait avoir comme conséquence que «[l'intelligence artificielle] identifie ce qu'elle croit être du contenu visé par la loi et envoie un rapport à la GRC» [7] – augmentant encore plus la surveillance et le contrôle disproportionnés par la police des communautés colonisées et racisées. [8]

4) Les pouvoirs de fouille très larges accordés à des «inspecteurs» chargés de vérifier la conformité avec la loi, les audiences secrètes, les nouveaux pouvoirs de collecte d'information accordés au SCRS – lui octroyant davantage de pouvoirs similaires à ceux de la police.

5) Le manque de transparence, de reddition de compte, de recours et de mécanisme public pour évaluer si les compagnies Internet respectent leur obligation de traitement non-discriminatoire lorsqu'elles retirent du contenu et font rapport aux forces policières et au SCRS; la protection accordée à ces compagnies qui sont à l'abri de poursuites civiles et criminelles lorsqu'elles rapportent «de bonne foi» à la police ou au SCRS; le manque d'obligation qu'ont les compagnies de restaurer le contenu supprimé à tort et qui sont libres d'appliquer leurs propres standards de communauté. Comme l'ont souligné récemment trois rapporteur.es de l'ONU, «ces standards ne font pas référence aux droits humains et aux obligations qui en découlent, ce qui crée la possibilité d'échapper à la reddition de compte en matière de droits de la personne.» [9]

Selon Daphne Keller, directrice du Program on Platform Regulation au Stanford's Cyber Policy Center, la proposition du Canada constitue une «liste des pires idées qui ont cours dans le monde – celles que les organisations de défense des droits humains ont combattu à l'Union européenne, en Inde, en Australie, à Singapour, en Indonésie et ailleurs.» [10]

Les lacunes troublantes dans le processus de consultation visant à valider ce projet de loi ne font qu'augmenter nos préoccupations. Les points de vue d'expert.es sur comment s'attaquer aux contenus préjudiciables tout en respectant les libertés civiles ont été ignorés. [11] En raison des élections, les rencontres de consultation avec des représentant.es des communautés ont été annulées sans que la date de la fin des consultations, le 25 septembre – 5 jours après les élections – ait été repoussée.

Étant donné les risques sérieux que pose cette législation – y compris pour les communautés qu'elle est supposée protéger – nous demandons au gouvernement d'en suspendre la mise en œuvre tant qu'une consultation ouverte, complète et juste avec des expert.es en matière d'anti-racisme, de droits humains et de libertés civiles n'aura pas eu lieu, et que les problèmes et écueils identifiés ci-haut n'auront pas été corrigés.

### Organizations

Arab Canadian Lawyers Association British Columbia Civil Liberties Association Canada Palestine Association Canada Palestine Support Network - CanPalNet **Canadian BDS Coalition** Canadian Council of Muslim Women (CCMW) **Canadian Foreign Policy Institute** Canadians for Justice and Peace in the Middle East (CJPME) Canadians for Peace and Justice in Kashmir (CPJK) **Canadians United Against Hate** Catholics for Justice and Peace in the Holy Land Community Coalition Against Racism (Hamilton) Independent Jewish Voices Canada / Voix juives indépendantes (IJV) International Civil Liberties Monitoring Group (ICLMG) Islamic Social Services Association Jewish Liberation Theology Institute Just Peace Advocates/Mouvement Pour Une Paix Juste Ligue des droits et libertés Mathabah Institute Niagara Movement for Justice in Palestine-Israel (NMJPI), ON Canada

tan sheriyeda eskeriyetin ya san san san sa Sarye ana ana san san san bahaying bar Kenang maka akan san san gana na san Restera (Marcanta) san san san san san sa

PAJU (Palestinian and Jewish Unity) Palestinian Canadian Congress Samidoun Palestinian Prisoner Solidarity Network Sisters Dialogue Socialist Action / Ligue pour l'Action socialiste South Asian Legal Clinic of Ontario Uyghur Rights Advocacy Project

### Individuals

Aman Sium, Eritreans for Peace and Justice

Anna Lippman, PhD candidate

Anne Dagenais, activist

Annette Lengyel, Human Rights for Palestinians Activist

Aron Rosenberg, PhD Candidate, McGill University

Dr Arun Kundnani, writer

Azeezah Kanji, journalist and legal academic

Bill Skidmore, Human Rights professor, Carleton University (retired)

Dr Chandni Desai, Assistant Professor, Critical Studies of Equity and Solidarity, University of Toronto

Cheryl Gaster, Human Rights Lawyer (Retired)

Claudia K. Keller, Clergy

Corey Balsam, National Coordinator, Independent Jewish Voices

Dania Majid, Arab Canadian Lawyers Association

Dr David Palumbo-Liu, Louise Hewlett Nixon Professor, Stanford University., US D Nashi, Barrister and Solicitor

Doug Hewitt-White, Conscience Canada

Dr. Adnan A. Husain (Department of History and Director, Muslim Societies-Global Perspectives Project, Queen's University)

Dr. James Deutsch, Div. of Child and Adolescent Psychiatry, Univ. of Toronto

landa bahasha da Majji san Sunda Guye ang ang Sun Olikoma bah Kasan saka kasan kang ang sun Rester 1955 ng saka sakang sung su

Dr. Sujith Xavier, Associate Professor, Faculty of Law University of Windsor

Ed Corrigan, lawyer

Elizabeth Block, member of Independent Jewish Voices and CFSC

Elizabeth-Anne Malischewski, Independent Jewish Voices

Emo Yango, The United Church of Canada

Ernest Dalymple-Alford, retired university professor

Faisal Bhabha, Associate Professor, Osgoode Hall Law School, York University

Gail Nestel, Educator

Gordon Doctorow, Ed.D.

Greg Starr, College Instructor

Helga Mankovitz, member, Independent Jewish Voices

Jeannette Schieck, BA MSc retired OCT

Dr Jeffrey Monaghan, Associate Professor, Carleton University

Jenny Stimac, Independent Jewish Voices

Jeremy Wildeman, PhD

Jillian Rogin, Assistant Professor, University of Windsor, Faculty of Law

Karen Rodman (Rev), ordained minister and human rights advocate

Karin Brothers, writer and activist

Khaled Loutfi Mouammar, Former Member of the Immigration and Refugee Board of Canada

Kikélola Roach, Unifor National Chair in Social Justice and Democracy at X University (formerly Ryerson)

Lev Jaeger, United Jewish People's Order member, Independent Jewish Voices member

Dr Mark Ayyash, Associate Professor of Sociology, Mount Royal University

Mark Robert Brill, member, Independent Jewish Voices, Ontario Coalition Against Poverty, long time activist

Mary Girard, human rights and justice activist

Michael Keefer, Professor Emeritus, University of Guelph

Dr Nahla Abdo, Professor, Carleton University

Nicholas Sammond, Director, Centre for the Study of the United States, University of

tensta sent este statut (E. an. Consta Receive accenter Science) al constant Receive activité de la constant (E. an. Receive activité de la constant (E. an. Constant) Receives de la constant (E. an. Constant)

Toronto Omar Burgan, Labour researcher Dr Paola Bacchetta, Professor, University of California, Berkeley Parker Mah, community activist Rabbi David Mivasair, emeritus, Ahavat Olam Synagogue Rachel Small, World BEYOND War Dr Randa Farah, Associate Professor, WesternU Rashmi Luther, Lecturer (retired), School of Social Work, Carleton University Ria Heynen, activist **Richard Marcuse**, Arts Consultant Dr Rinaldo Walcott, Associate Professor, University of Toronto Sam Arnold, Independent Jewish Voices Shawn Nock, human rights activist Sid Shniad, solidarity activist, member Independent Jewish Voices Canada Suzanne Weiss, author and activist Sydney Nestel, IT consultant, retired Tim McSorley, National Coordinator, International Civil Liberties Monitoring Group Vicki Obedkoff, United Church of Canada minister Wolfe Erlichman, Independent Jewish Voices Yom Shamash, Independent Jewish Voices Zainab Amadahy, author and community activist

### September 25, 2021

s.19(1)

#### To Whom It May Concern:

I am writing with respect to the government's proposed approach to address harmful content online. I am a Canadian

### I am writing this letter in my individual capacity.

First, I would like to thank you for taking this issue seriously. Even though much of this content is already illegal in Canada, further reducing its proliferation online is a worthy goal. As you are no doubt aware, governments around the world, and particularly in Europe, have introduced legislation to combat these harms. Even in the United States, where First Amendment free speech protections are near-absolute, the distribution of child sexual abuse material is a federal crime and inciting violence can trigger serious criminal penalties. I applaud the government in seriously studying these issues and leading the way in reducing online harms even further.

Yet I am concerned with some aspects of the proposed legislation. Some of these ideas have been vigorously protested by human rights organizations and struck down as unconstitutional in liberal democracies around the world. In this letter, I would like to flag a few concerns, hoping to help you navigate the delicate balance between free expression rights and other important protections.

As I am sure you recognize, proactive monitoring of user speech presents privacy issues. Under European law, national governments may not impose an obligation on online platforms to monitor user content, nor an obligation to actively seek facts or circumstances indicating illegal activity. Without restrictions on proactive monitoring, national governments would be able to significantly increase their surveillance powers. The *Canadian Charter of Rights and Freedoms* protects all Canadians from unreasonable searches. But under the proposed legislation, a reasonable suspicion of illegal activity would not be necessary for a service provider, acting on the government's behalf, to conduct a search. All content posted online would be searched. Potentially harmful content would be stored by the service provider and transmitted—in secret—to the government for criminal prosecution.

Importantly, Canadians who have nothing to hide would still have something to fear. Social media platforms process billions of pieces of content every day. Proactive monitoring is only possible with an automated system. Yet automated systems are notoriously inaccurate. Facebook, which runs one of the most advanced artificial intelligence research labs in the world, employs over ten thousand human content reviewers because it cannot build sufficiently accurate algorithms to replace them. And even the human content reviewers make mistakes. Some reports indicate Facebook has a manual content moderation accuracy target of 95% but achieves accuracy below 90%. Social media companies are not like newspapers; accurately reviewing every piece of content is operationally impossible. The outcome is uncomfortable: Many innocent Canadians will be referred for criminal prosecution under the proposed legislation.

But it gets worse. Individual pieces of user-generated content are worth little to online communication service providers. Instagram does not make much money from a picture of one's lunch. But if an online communication service provider determined that one's content was not harmful within the tight twenty-four-hour review period, and later the government decided otherwise, the provider would lose up to three percent of their gross global revenue. Accordingly, any rational platform would censor far more content than illegal. After all, given the size of the potential penalty, taking even a small risk would be a poor business decision. Human rights scholars call this troubling phenomenon "collateral censorship."

The twenty-four-hour removal provision for illegal speech is identical to *Loi Avia*, a French statute struck down by France's Constitutional Council in 2020. France has strict limits on freedom of expression. For instance, thousands of people are convicted each year for the vaguely defined offense of "contempt of public officials," which criminalizes insulting politicians. Amnesty International has also called France's record on freedom of expression "bleak." But even for France, which has some of the toughest hate speech restrictions in the world, the risk of collateral censorship was too high for *Loi Avia* to pass constitutional muster. In Germany, NetzDG gives platforms seven days to carefully assess whether speech is illegal and even that timeline generated significant concern from human rights scholars.

Identifying illegal content is difficult, and therefore the risk of collateral censorship is high. Consider a seemingly obviously illegal category of content: child sexual abuse material. Is Nirvana's famous album cover that includes a naked baby an example of child pornography? What about a photograph you took of your topless child at the pool to share with your family? Would Facebook be willing to risk almost three billion dollars by not reporting such content for criminal prosecution? When the moderation decision requires even a moment's thought, censorship is guaranteed.

Hate speech restrictions may best illustrate the problem. The proposal expects platforms to apply the Supreme Court of Canada's hate speech jurisprudence. Identifying hate speech is difficult for courts, let alone algorithms or low-paid content moderators who must make decisions in mere seconds. Although speech that merely offends is not hate speech, platforms are likely to remove anything that has even the slightest potential to offend.

As the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has explained, "hate speech" is a vague concept that conventional international law does not define. The United Nations has expressed concern that many governments use "hate speech" to attack political enemies, non-believers, dissenters, and critics. While the risk of this occurring in Canada are low, governments who consistently infringe their citizens' human rights would love to point to a Canadian law as justification for their own similar legislation. Canadians, unlike many others, are protected from government abuse of restrictions on free expression because of our judicial system's strong due process guarantees. Social media platforms, who process billions of pieces of content each day, are unable to provide similar protections.

Unfortunately, these are other issues. I am concerned that a new Digital Safety Commissioner may require any online content service provider to do "any act or thing" to ensure compliance. The Commissioner may enter into a coercive "compliance agreement" that may require platforms to take actions aside from reducing online harms to avoid significant monetary penalties. This is a power that requires oversight. But the proposed legislation allows for secret hearings. In some cases, the government may order an entire website to be taken down even if the vast majority of content hosted by it is legal. These powers are ripe for abuse. In most liberal democracies, such legislation would be blatantly unconstitutional. When the United States tried to pass legislation that would have allowed regulators to take down entire websites for some instances of copyright infringement, the government was heavily criticized by the United Nations for threatening innocent users' human right to free expression. The Canadian government's proposal goes much further.

Even though right-wing speakers often claim they are being censored online, it's worth highlighting that this not a partisan issue. I have seen many examples of left-leaning content taken down that is wholly unproblematic. This content is not just legal, but clearly inline with platform policies. This censorship infuriates Canadians every day. There is obviously much *illegal* content that should be removed from the Internet. But legislation must be very carefully drafted so platforms are not given a strong incentive to take down wholly *legal* content. The current draft does not pass this critical test.

Regulating online harms is a serious issue that the Canadian government, like all others, must tackle to protect its citizens. Child pornography, terrorist content, incitement, hate speech, and revenge pornography has no place in Canada. To a large degree such content is already illegal. Still, we need to ensure there is less of this content online. And effective policy can do that. But this proposal, as currently drafted, brings great risks. No other liberal democracy has been willing to accept these risks.

I am happy to discuss this further and offer additional thoughts. I am also happy to introduce you to people within the

keeping Canadians sate online is an issue I care much about. And I thank you again for devoting time to finding a solution.

s.19(1)

Thank you,

Alan Kogan

Ilan Kogan

Toronto, Canada

Gostammet commonique en variar es la Ero aver concesa à l'information Document indesent concount fo ille Access la information a ri

# ACTION COALITION

September 25, 2021

We, the Sex Workers of Winnipeg Action Coalition would like to explicitly state our opposition to the approach and content presented in the discussion and technical papers related to moderation of Online Communication Services.

It's difficult to come forward to seemingly argue against horrific acts such as revenge porn, exploitation, terrorism, and hate speech. Please trust that we share the feelings of the vast majority of humans that these are reprehensible acts, and we stand against them. However, we need you to understand that this particular method of attempting to achieve a safer internet is actually one that will cause a great deal of harm.

We have been following part of this discussion — specifically concerned with dissemination of sexually explicit materials from the ETHI committee's Protection of Privacy and Reputation on Platforms such as the PornHub discussions. We would like to make it abundantly clear that, although the committee's final report paid a large amount of lip service to consultation with sex worker groups, that our voices were barely let into the conversation, were denied their full character, and even outright ignored.

As discussed in our brief to the ETHI committee, additional scrutiny on sex workers' ability to exist online is directly in opposition to our ability to keep safe and conduct our legal work safely. Because of the unreasonably short time period allowed for a website to filter content, the practical result of these recommendations will be the filtering out of all content that is deemed to be sexual in nature, regardless of whether it was consensual or not. The risks are too high for any company to take chances, and they will enact sweeping filters on keywords and content types, as we've already seen in the United States with their introduction of SESTA/FOSTA (which is now being challenged in American courts).

> SWWAC c/o 646 Logan Ave, Winnipeg MB R3A 057 Enrall: swwac@sexworkwinnipeg.com Facebook: <u>https://www.facebook.com/SWWACwpg/</u> Twitter: <u>@SWWACwpg</u>

We point to the hard data that shows the related decrease in femicide when sex workers were allowed to use online services to set up their work<sup>1</sup>, and the associated flip back that has begun since SESTA/ FOSTA shut down sites like Backpage and Craigslist's adult services pages<sup>2</sup>. The groups whose voices were most heard at the ETHI committee's hearings insist that lives will be saved with these new recommendations, but we have proof that the opposite is true.

To put it bluntly, when sex workers do not have safe spaces to advertise their own services, form community and connections, and have access to peer-led safety services like Bad Date lists (which serve to warn sex workers of abusers, people who don't pay, people who are coercive, vehicles that are harassing workers, etc), we die. There is no sugar-coating this, and you must confront this as a reality.

Governments have a duty to make law and policy that will not interfere with the rights of any Canadian to express themselves, to not be discriminated against, to live their full lives. The scope of the recommendations on identification and storage of IP addresses is far too vast and riddled with opportunities for identity theft, stalking, blackmail, and more.

The duty to make law and policy that will not later be easily misused by any government also applies in this case. The sort of access to personal identity around online posting concerns us as it relates to policing and surveillance of sex workers, as well as freedom of expression of all those in Canada. This will undoubtedly disproportionally affect the most marginalized people (folks of colour, 2SLGBTTQ individuals, and their intersection). These sorts of sweeping and fundamental changes to privacy online can be easily abused by future governments hoping to silence dissenting voices, or track down sex workers, for example. This flies in the face of freedom of expression, and is incredibly worrying.

There is no need for additional carceral language in our lawmaking against violent people. Laws already exists against all of the five harms mentioned in the discussion and technical papers. In the case of the ETHI committee's witness statements, we know who all of those perpetrators of violence were. We have their identities, we know who they are. The proposed changes do nothing to address why these people commit these acts of violence, and nothing to ensure that they can be brought to justice. And yet we aren't having the conversation of how to ensure that people's lives, careers, hopes

<sup>&</sup>lt;sup>1</sup> The Effect of Online Erotic Services Advertising on Prostitution Markets, Pricing, and Murder: Cunningham et al. 2017 <u>https://cear.gsu.edu/files/gravity\_forms/</u> 45-9a8e751f713c799256f347c4aad2a49d/2017/04/Online-Erotic-Services-Advertising-and-Murder.pdf

<sup>&</sup>lt;sup>2</sup> Craigslist's Effect on Violence Against Women: https://www.documentcloud.org/documents/ 4442319-Craigslist-s-Effect-on-Violence-Against-Women.html

and dreams aren't dashed if they are a victim of revenge porn or non-consensual sharing of images on the internet. We are instead talking about overstepping privacy for every person in Canada.

The organizations leading the charge for the ETHI committee do not have Canadian values of diversity, inclusion, and care at heart. Many of these organizations state explicitly that marriage is meant to be between one man and one woman, sex is determined at birth, and a great number of them explicitly state that all online sexually explicit media is necessarily exploitation. Their web pages have links to pages where one can learn to pray for the end of all pornography. These opinions go against the very values that most Canadians hold and that are protected in the Canadian Charter of Rights and Freedoms. Prohibition is their goal.

We know from experience – and ever-growing peer-reviewed evidence – that prohibition of sex work kills, and specifically kills women and 2SLGBTTQ folks. We said it in our initial brief to the ETHI committee and we will say it as loudly and as often as it needs to be said. Prohibition not only does not work, but it kills. Please see also: the war on drugs, prohibition of alcohol, sex work policing in metro Vancouver, the Bedford decision, etc.

Prohibition also leaves society in a place where abusive acts like revenge porn still have power over their victims by reinforcing sexuality as unfit for public view. The more shameful we make sexuality, the worse things are for victims. The more we allow powerful groups such as employers, education systems, and even parents to feel emboldened to shame victims, the more harm is done.

The sanctions involved in these recommendations will also deter smaller, more ethically-operated companies from getting started in the adult realm. It will kill small businesses, deplatform individuals working for themselves on the internet, and only ensure the success of the monopoly of PornHub/ Mindgeek.

We would also like to point out that, while the final report of the ETHI committee thanked five revenge porn victims that came forward with briefs and witness statements, there were at least six revenge porn victims who relived their abuses for the committee. The one the committee left out was a sex worker's story of resilience after abuse. This was not accidental. We want to draw specific attention to that intentional omission and how it blatantly contradicts the same report's claims that sex worker voices would be considered. It is clear to us that they were not given the same priority, as the committee stripped that witness of her own victimhood.

We urge you to slow this discussion down, and genuinely engage with sex workers about how this sort of knee-jerk, over-reaching policymaking will cost lives. Canadian sex workers are eager to contribute our expertise to combat horrific acts such as revenge porn, exploitation, terrorism, and hate speech. This can easily be seen by how, despite the seemingly universal refusal to include our voices, we are still writing briefs and contributing in whatever way we can. We have been doing our part and sharing our experience, now you need only have the meaningful conversations with us. Please remember that sexually explicit material is legal, and people engaging consensually in it online should not be criminalized, marginalized, or silenced for their choice to participate in it.

Prohibition doesn't make difficult issues go away. It only makes them less safe.

Environmentering son sonder Expression de Arts Folkonnelsen Romannelsenkonnelsen aussieren Die Stereits den internetsen

### Comments of Electronic Frontier Foundation re: Proposed Framework to Address Harmful Content

Digital Citizen Initiative Department of Canadian Heritage via email: <u>pch.icn-dci.pch@canada.ca</u>

> Corynne McSherry Legal Director, EFF

> September 25, 2021

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. With over 30,000 dues-paying members – including several hundred Canadian residents—and more than 1 million followers on social networks, we focus on promoting policies that benefit internet users.

For nearly 30 years, EFF has represented the interests of technology users both in court cases and in broader policy debates to help ensure that law and technology support our civil liberties. We are well aware that online speech is not always pretty—sometimes it's extremely ugly and causes real-world harm. The effects of this kind of speech are often disproportionately felt by communities for whom the internet has also provided invaluable tools to organize, educate, and connect. Systemic discrimination does not disappear and can even be amplified online. Given the paucity and inadequacy of tools for users themselves to push back, it's no surprise that many would look to internet intermediaries to do more to limit such speech.

However, the framework outlined in the discussion guide and technical paper would be a genuine disaster for online expression and access to information. Particularly dangerous elements include:

- a 24-hour takedown requirement that will be far too short for reasonable consideration of context and nuance;
- the effective filtering requirement (the proposal says service providers must take reasonable measures which "may include" filters, but, in practice, compliance will require them);
- penalties of up to 3 percent of the providers' gross revenues or up to 10 million dollars, whichever is higher;
- mandatory reporting of *potentially* harmful content (and the users who post it) to law enforcement and national security agencies;
- website blocking;
- · onerous data-retention obligations

The most dangerous aspect of the proposal, however, it that it would create a new internet speech czar with broad powers to ensure compliance–including via inspection and seizure—and continuously redefine what compliance means.

The potential harms here are vast, and they'll only grow because so much of the regulation is left open. In the United States and elsewhere, we have seen how rules like those proposed here hurt marginalized groups, both online and offline. Faced with expansive and vague moderation obligations, little time for analysis, and major legal consequences if they guess wrong, companies inevitably overcensor—and users pay the price. For example, a U.S. law intended to penalize sites that hosted speech related to child sexual abuse and trafficking led large and small internet platforms to take down broad swaths of speech with adult content. The consequences of have been devastating for marginalized communities and groups that serve them, especially organizations that provide support and services to victims of trafficking and child abuse, sex workers, and groups and individuals promoting sexual freedom. Taking away online forums, client-screening capabilities, "bad date" lists, and other intra-community safety tips means putting more workers on the street, at higher risk, which leads to increased violence and trafficking. The impact was particularly harmful for trans women of color, who are disproportionately affected by this violence. <sup>1,2,3</sup>

Indeed, even "voluntary" content moderation rules are dangerous.<sup>4</sup> For example, policies against hate speech have shut down online conversations about racism and harassment of people of color. Ambiguous "community standards" have prevented Black Lives Matter activists from showing the world the racist messages they receive.<sup>5</sup> Rules against depictions of violence have removed reports about the Syrian war and accounts of human rights abuses of Myanmar's Rohingya.<sup>6,7</sup> These voices, and the voices of aboriginal women in Australia, Dakota pipeline protestors and many others, are being erased online. Their stories and images of mass arrests, military attacks, racism, and genocide are being flagged for takedown. What is worse, compliance with the proposal here will likely require the use of automated filters to assess and discover "harmful" content on their platforms. Such filters inevitably sweep in lawful content. <sup>8</sup>

The powerless struggle to be heard in the first place; the government's proposal will make it harder for them to take full advantage of online forums as well.

That's one reason human rights defenders, the UN, and a wide range of civil society groups have criticized similar policies in other countries. For example, the content monitoring obligations echo proposals in India and the UK that have been widely criticized by civil society, not to

https://appam.confex.com/appam/2014/webprogram/Paper11163.html

<sup>&</sup>lt;sup>2</sup> https://swopusa.org/blog/2015/11/12/trans-day-of-remembrance-statement-fact-sheet/

<sup>&</sup>lt;sup>3</sup> https://www.huffpost.com/entry/opinion-butler-fosta-sex-work\_n\_5ad75366e4b0e4d0715c4bf8

<sup>&</sup>lt;sup>4</sup> https://www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes

<sup>&</sup>lt;sup>5</sup> https://www.theguardian.com/technology/2016/sep/12/facebook-blocks-shaun-king-black-lives-matter

<sup>&</sup>lt;sup>6</sup> https://www.nytimes.com/2017/08/22/world/middleeast/syria-youtube-videos-isis.html

<sup>&</sup>lt;sup>7</sup> https://www.thedailybeast.com/exclusive-rohingya-activists-say-facebook-silences-them

<sup>8</sup> https://www.eff.org/tossedout/tumblr-ban-adult-content

mention three UN Rapporteurs.<sup>9,10,11</sup> It would import the worst aspects of Germany's Network Enforcement Act, ("NetzDG"), which deputizes private companies to police the internet, following a rushed timeline that precludes any hope of a balanced legal analysis, leading to takedowns of innocuous posts and satirical content.<sup>12,13,14</sup> The law has been heavily criticized in Germany and abroad, and experts say it conflicts with the EU's central internet regulation, the E-Commerce Directive. It also bears a striking similarity to France's "hate speech" law, which was struck down as unconstitutional.<sup>15,16</sup>

Further, the framework is inconsistent with Canada's trade obligations. Article 19.17 of the USMCA prohibits treating platforms as the originators of content when determining liability for information harms.<sup>17</sup> But this proposal does precisely that—in multiple ways, a platform's legal risk will depend on whether it properly identifies and removes harmful content it had no part in creating.

There is yet another problem: the regulatory scheme would depart from settled human rights norms. The UN Special Rapporteur on free expression has urged that states should only seek to restrict content pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality, necessity and legitimacy. The Rapporteur also called upon companies to recognize human rights law as the authoritative global standard for freedom of expression on their platforms. Canada should not force companies to violate human rights law instead.<sup>18</sup>

Finally, we note that the proposal would further entrench the power of U.S. tech giants over social media, because they are the only ones who can afford to comply with these complex and draconian obligations.

This proposal is dangerous to online expression and competition. We urge you to reject it entirely.

<sup>10</sup> https://www.eff.org/deeplinks/2021/07/uks-draft-online-safety-bill-raises-serious-concerns-around-freedom-expression

<sup>11</sup> https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=26385

12 https://www.hiig.de/wp-content/uploads/2018/07/SSRN-id3216572.pdf

<sup>13</sup> https://www.techdirt.com/articles/20180217/19141939260/germanys-speech-laws-continue-to-beraging-dumpster-fire-censorial-stupidity.shtml

<sup>14</sup> https://www.techdirt.com/articles/20180105/15544738943/it-took-only-three-days-germanys-new-hate-speech-law-to-cause-collateral-damage.shtml

<sup>15</sup> https://www.jipitec.eu/issues/jipitec-8-2-2017/4567

<sup>16</sup> https://www.eff.org/press/releases/victory-french-high-court-rules-most-hate-speech-bill-wouldundermine-free-expression

<sup>17</sup> https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf

18 https://freedex.org/a-human-rights-approach-to-platform-content-regulation/

## TikTok's Submission to the Department of Canadian Heritage on the *Government's Proposed Approach to Address Harmful Content Online*

Submitted via email to: Department of Canadian Heritage pch.icn-dci.pch@canada.ca

September 25, 2021

HE METERS TO OTOMOTOMICS

ikTok

### Introduction

TikTok values the opportunity to respond to the Government of Canada's *proposed approach* to address harmful content online ("the Proposal"). We support and share the Government's objective of combatting hate speech and other kinds of harmful content online, and believe that government, industry, and civil society all play a crucial role in taking meaningful action to further combat harmful content.

It is our view that user-generated content platforms should operate within a clearly defined legal framework established by Parliament. Moreover, the intentions behind this Proposal reflect TikTok's own prioritization of safety. Ensuring a safe and secure environment for our users is a top priority for TikTok, both now and after any new legislation is passed and comes into effect.

Our intention in this submission is to reflect these principles and highlight where further clarity is needed at this stage, to discuss where there are potential gaps or conflicts in the Proposal that could undermine its intended impact, and to address certain practical challenges that we have identified in the implementation of the Proposal. The feedback and concerns identified in this submission are not exhaustive, and we look forward to the continued opportunity to engage with you on the development of the Proposal.

### About TikTok Canada

TikTok is a global entertainment platform where people create and watch short-form videos. Our mission is to inspire creativity and bring joy. For TikTok, creative ideas matter more than social connection, and people on the platform are celebrated for being their authentic selves. TikTok videos tend to be light-hearted, real, heart-warming, and truly fun.

TikTok opened its Canadian office in late 2019, and we have since grown to over 50 employees focused on supporting Canadian creators, artists, small businesses, and brands. Our goal is to help these Canadian creators connect authentically with audiences and customers across Canada and around the world. Canadians of all backgrounds, young and old, and from all provinces and territories use TikTok to express themselves creatively and openly, and to share their lives, talents, and humour. We are especially proud of the communities that have been formed on our platform by Indigenous, LGBTQ2S+, racialized, and other equity-deserving groups who in the past have not been represented in traditional Canadian media. We are proud to provide a platform where all Canadians can share their ideas and culture on a global stage.

### TikTok's Approach to User Safety

The safety and security of our users is a top priority for TikTok, and we have invested significant resources into keeping our platform safe by effectively identifying and removing harmful content uploaded to our platform. Our approach to safety is built upon a "Three P's" approach, which includes our policies, product, and partners:

### Policies

TikTok's Community Guidelines and Terms of Service reflect our values and establish the kind of behaviour we expect from our community of users. Our users devote significant time and creativity to making content for TikTok, and it's critical to us that our systems for moderating content are accurate and consistent. Our Community Guidelines reflect this driving philosophy – providing a platform for creative self-expression while remaining safe, diverse, and authentic – and define a common code of conduct on our platform.<sup>1</sup> Our team of policy, operations, safety, and security experts work together to develop equitable policies that can be consistently enforced. Our policies take into account a diverse range of feedback we gather from external experts in digital safety and human rights.

We proactively enforce our Community Guidelines using a mix of technology and human moderation. Content uploaded to TikTok initially passes through technology that works to identify and flag potential policy violations for further review by a safety team member. We also encourage users to report content that they think violates the Community Guidelines, which can be reported easily within the app, and is then reviewed by our safety team. In some cases where our technology has a high degree of accuracy (such as minor safety, adult nudity and sexual activities, and violent and graphic content), violative content will be removed automatically upon upload.

Videos that are found to violate our guidelines are removed and the creator is notified of the removal and reason, and given the opportunity to appeal the removal. When we receive an appeal, we review the video a second time and will reinstate it if it is found not to violate our policies.

It is our policy to remove any content – including video, audio, livestream, images, comments, and text – that violates our Community Guidelines. We will suspend or ban accounts and/or devices that are involved in severe or repeated violations, and we will consider information available on other platforms and offline in these decisions. When warranted, we will report the accounts to the appropriate legal authorities.

### Product

We take an upstream, safety by design approach to protect our users' safety and wellbeing, helping to promote safe and positive experiences on our platform. Some examples of these features include:

- Youth Safety: We create age-appropriate environments by implementing strong default privacy settings for users under 18, disabling features like direct messages, duet/stitch, downloading of videos, and livestreaming for all users under 16. We also enable parents to set guardrails on their teens' account by using our Family Pairing feature. We actively promote these features to our users to ensure they have a genuine impact.
- Wellbeing: We prompt users to ask them to consider the impact of their words if they post a potentially unkind comment, and allow users to filter, delete, or report comments, and block users in bulk, so that only comments they approve appear in their videos. We also redirect searches and hashtags that indicate a person

The ARTIST TO OTHER MADE

ikTok

Community Guidelines, https://www.tiktok.com/community-guidelines

may be struggling with self-harm behaviour, thoughts of suicide, or an eating disorder to local help lines.

Misinformation: We remove misinformation as we identify it, but when fact checks are inconclusive or content is not able to be confirmed (especially during unfolding events) a video may become ineligible for recommendation into anyone's feed (For Your Page). We will prompt users who attempt to share these videos to remind them that the video's contents are unverified, and ask them to reconsider before sharing.

### Partners

We constantly seek to build partnerships with local organizations and stakeholders, whose input and feedback make our policies, products, and safeguards stronger and more comprehensive for our community. In Canada, we work with leading issue experts and safety organizations including MediaSmarts, Kids Help Phone, the National Eating Disorder Information Centre, the Native Women's Association of Canada, YWCA Canada, and many others to inform our policies, product features, and user resources, and to ensure that local dynamics and cultural context are incorporated into our safety efforts.

We also partner with all levels of government to support the communication of important public service announcements, such as public health information related to COVID-19. During the recent federal election, we worked with Elections Canada to counter election misinformation by creating a bilingual in-app Election Guide that provided users with verified information on when and how they could vote.<sup>2</sup> This year, TikTok was proud to sign the Canada Declaration on Electoral Integrity Online, where we committed to working with the federal government to support healthy and safe democratic debate and expression online.<sup>3</sup>

In all our safety endeavours, we strive to be transparent about how we enforce our policies so as to continue building trust with our community members. We believe that transparency and accountability are essential cornerstones of enabling trust with our users, and that all companies should be in a position to explain their recommendation algorithms and moderation policies to regulators.

To put this belief into action, in 2020 we opened a Transparency and Accountability Centre where policymakers and experts can observe our moderation policies in real-time and examine the actual code that drives our algorithms.<sup>4</sup> During the pandemic, we've provided a virtual version of this tour, including to Canadian officials. The Transparency and Accountability Centre builds on work that we are already doing to increase visibility into how our platform operates, including publishing regular Transparency Reports<sup>5</sup> and sharing more about how we recommend content.6

There is no finish line when it comes to protecting the TikTok community. We work each day to learn, adapt, and strengthen our policies and practices to keep our community safe.

tree contains at 10060708 butter

THE METERS TO OTIO20120020

**cTok** 

<sup>&</sup>lt;sup>2</sup> TikTok launches in-app guide for Canada's federal election, https://newsroom.tiktok.com/en-ca/tiktok-launches-in-app-guidefor-canadas-federal-election

<sup>&</sup>lt;sup>3</sup> Canada Declaration on Electoral Integrity Online, https://www.canada.ca/en/democratic-institutions/services/protecting-

democracy/declaration-electoral-integrity.html An update on our virtual Transparency & Accountability Center experience, https://newsroom.tiktok.com/en-us/an-update-onour-virtual-transparency-and-accountability-center-experience <sup>5</sup> Transparency at TikTok, <u>https://www.tiktok.com/transparency</u>

<sup>6</sup> How TikTok recommends videos #ForYou, https://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you

### Comments on the Proposal

**General Comments:** TikTok commends the Proposal's adoption of a systemic regulatory framework that looks at systems and processes rather than individual pieces of content. We believe this is a proportionate, consistent, and fair approach and it specifically recognizes the different nature of platforms and the rapidly evolving technological environment. Crucially, it helps to future proof the legislation, and allows for new innovations, platforms, and apps currently not on the market.

### Section 1: Legislative Premises

Globally in the first quarter of 2021, content that violated our Community Guidelines or Terms of Service accounted for less than 1% of all videos uploaded on TikTok. Of the videos removed, we identified and removed 91.3% before a user reported them, 81.8% before they received any views, and 93.1% within 24 hours of being posted.

Content that violates TikTok's policies comprises a very small percentage of the total videos uploaded by users – and an even smaller fraction would be considered "harmful content" within the scope of this Proposal. Recognizing in the Act's preamble that the vast majority of content posted by and accessible to Canadians on platforms like TikTok is not harmful would reinforce the importance of respecting the fundamental of rights and freedoms of Canadians when interpreting the provisions of the Act.

### Section 8: Definitions of Harmful Content

We support the Proposal's focus on illegal content, as this is where we as a platform operator can find the most certainty. We are able to quickly and accurately remove violative content when our moderators have clear, specific, and behavioural-based guidelines that allow them to evaluate content based on the information available to them. The Proposal's references to external statutes and case law within the definitions of certain categories of harmful content would cloud the certainty with which our moderators can make these determinations. For example, the Proposal's definition of hate speech incorporates decades of Supreme Court of Canada jurisprudence, which would require our content moderators - who must make decisions based on what information is available to them in a video - to apply a judicial test that requires them to be "aware of the relevant context and circumstances"<sup>7</sup> in which a statement was made.

We strongly urge the government to work with platforms to collaboratively develop workable definitions of harmful content that are clear, enforceable, and scalable, and which will provide us with the most certainty when evaluating content under the Act. We also recommend using the term "illegal content" instead of "harmful content" throughout the Act to reinforce the legislation's limitation in scope to the five defined categories of illegal content.

### Section 11: Timelines for Actioning Content

We understand the desire for prescribing specific, short timelines for actioning flagged content. While we work 24/7 to moderate content uploaded to our platform, we believe that it is critical that we get our moderation decisions right -- and not rush to make a rapid decision without assessing all the available facts. This is particularly important when we deal with complex, contextual cases that require thorough evaluation in order to avoid over moderation -- which has potential consequences for users' fundamental rights and freedoms.

Recognizing this important balance, other jurisdictions around the world have adopted more flexible timelines in similar frameworks: The European Commission's proposed Digital Services Act would require content to be removed in "a timely, diligent and objective

la car an car à d'Information 2010 anna Company anna an tao anna an 1110 Aire 220 an amhrann an A

ik Tok

<sup>&</sup>lt;sup>7</sup> Saskatchewan (Human Rights Commission) v. Whatcott, 2013 SCC 11, [2013] 1 S.C.R. 467

manner;" while the United Kingdom's draft Online Safety Bill does not adopt any specific timelines for actioning content, and rather focuses on ensuring that platforms have appropriate systems and processes in place. Even Germany's NetzDG regime provides seven days for a platform to respond to content where is it not "obviously illegal."

Instead of prescribing specific removal timelines, we recommend the Proposal adopt a flexible standard, such as "no undue delay," which would focus on ensuring that OCSPs have appropriate moderation policies, systems, and processes in place. This would reinforce the importance of accuracy and not just speed when reviewing potentially illegal content that requires further contextual of factual review.

### Section 14: Transparency Reporting

TikTok strongly supports the centrality of transparency reporting in the Proposal, which we agree is the appropriate mechanism for monitoring and measuring the success of platforms in enforcing the requirements of the Act. We currently release global reports on the enforcement of our Community Guidelines on a quarterly basis, and information related to law enforcement, government, and intellectual property removal requests bi-annually.

Producing comprehensive and accurate transparency reports is a highly resource intensive process. In light of the time and resources required to produce these reports, we request that reporting under this Proposal be required no more frequently than once every six months. We also request that OCSPs be given flexibility to choose the dates on which they submit their reporting, so long as it is provided within the required intervals. This would help ease the administrative burdens of preparing reports, as the timing could be coordinated with reporting for other regions.

We encourage the Government to consult with platforms to refine the categories of data proposed to be included in the reporting, and to align on meaningful reporting categories that will measure both the effectiveness of the platforms in enforcing the Act, and of the regulatory framework in reducing harmful content. Based on our platform operations, and how data is collected and analyzed, some of the categories in Section 14 would be too ambiguous to quantify or even impossible to measure. For example:

### a. the volume of harmful content on their OCS

The response would always be nil, as TikTok already does, and will continue to, remove any harmful content from our platform when it is identified.

### b. the volume and type of content that was accessible to persons in Canada in violation of their community guidelines

The scope should be focused on the five categories of harmful (illegal) content defined in the Proposal - and not a platform's broader community guidelines - to ensure that the data reported is relevant to compliance with the Act. The meaning of "was accessible" is also unclear as to whether it would include the significant percentage of violative content that is proactively removed after being uploaded but before it receives any views by users.

### c. the volume and type of content moderated;

It is unclear how this category differs from (b).

### f. how they monetize harmful content

The intended meaning of this is ill-defined and confusing.

e. their content moderation procedures, practices, rules, systems and activities, including automated decisions and community guidelines.

5

kTok

TikTok is prepared to go to great lengths to provide data access and to publish details about our practices and decisions, however, information in the wrong hands may have unintended consequences. Our publicly available Community Guidelines provide a comprehensive outline of what is and isn't allowed on our platform. However, training materials that explain how we identify violative content and apply our policies, in the wrong hands, would provide a blueprint for how to evade our policies and exacerbate the amount of violative material on our platform.

### h. (II) information about the kinds of demographics implicated [in reporting to law enforcement]

Consistent with privacy law principles, TikTok only requires that users provide limited information to use the service (such as date of birth and country location to confirm eligibility to use our app), and we do not require broader identifying information such as race, gender, or sexual orientation. Based on this approach, we would be very limited in our ability to provide any "information about the kinds of demographics implicated" in law enforcement reporting.

We also note that the list of reporting categories notably omits requiring data on the length of time taken to action harmful content following a user report, which is the central premise of the proposed framework.

### Section 20: Law Enforcement Reporting

TikTok is committed to cooperating with law enforcement while respecting the privacy and other rights of our users. We have internal policies and procedures governing how we handle and respond to law enforcement requests, and will only disclose user data where a request is based on a valid legal process or in emergency circumstances. Emergency circumstances mean an imminent harm or the risk of death or serious physical injury to a person.

Additional clarity is needed on the intended jurisdictional scope of the Section 20 proposals, particularly when a user's data is stored outside of Canada. Like other global platforms, TikTok operates a network of data centres in locations around the world where we securely store user data; TikTok's Canadian users' data is stored on servers in Singapore and the United States, and the TikTok app is provided to users in Canada by TikTok Pte Ltd., a Singapore-based entity. If we receive a request for user data or content from an authority located in a different country to the TikTok entity that provides the service to the user whose data is requested, we may require that a law enforcement authority submit a request for legal assistance to designated government authorities under the Mutual Legal Assistance Treaty ("MLAT") framework.

It is unclear how either of the proposed reporting obligations would interface with the MLAT processes that Canada has established with other countries. To protect privacy rights of Canadian and other users and ensure due process is followed, the Act should specify that when requiring the production of user data (including content) under either proposal in Section 20, law enforcement must provide valid legal process, including through an MLAT request when required, unless there is a specific and imminent threat of harm to an individual.

### Section 21: NCMEC Reporting

We strongly support the Proposal's reciprocal recognition of foreign statutory reporting requirements as deemed compliance with the Act, which would allow TikTok and other platforms to continue to utilize the well-established process for reporting child sexual abuse material (CSAM) to the National Center for Missing and Exploited Children (NCMEC) in the US. TikTok currently reports CSAM and predatory behavior found on the platform to NCMEC through their CyberTipline program. These reports are then forwarded by NCMEC to the RCMP's National Child Exploitation Crime Center (NCECC). This process allows for rapid and

Service and a service of Distribution and an internal services and the service of the DE Alexandry De antipological services

**kTok** 

streamlined reporting of CSAM to Canadian law enforcement by platforms located outside of Canada.

In order to ensure that the established NCMEC reporting process for platforms is not disrupted, we recommend that the Act's reporting requirements for CSAM be aligned to match NCMEC's eight categories of reportable content: suspected online enticement of children for sexual acts, child sexual molestation, child sexual abuse material, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet.<sup>8</sup>

### Sections 23-25: Preservation Requirements

Similar to the feedback provided above on Section 21, it's critical that the obligations being proposed for platforms to preserve user data be considered in a global context, and that the Act's preservation requirements be limited to Canadian user data. As written, Section 23 would require a OCSP to "preserve data and information in their possession pertinent to . . . potentially illegal content," with no geographic limit to the scope of this provision. This has the potential to create conflicts with the laws of other jurisdictions. For example, if applied to the data of an EU user, this requirement could conflict with EU law which imposes strict requirements around the disclosure, retention, and erasure of personal data that may differ from Canadian privacy law requirements.

### Sections 46-57: Digital Recourse Council of Canada

TikTok – as well as other major platforms – have invested extensively in building sophisticated content moderation teams that review millions of pieces of content every day. Creating a government-run Digital Recourse Council of Canada (DRCC), with the capacity to review complaints about content on *any platform* on the internet, would require mammoth budget and resources in order to service the likely volume of complaints, as well as expertise that doesn't currently exist within government. Rather than the government expending resources to duplicate the capacity and expertise that platforms have already built, we strongly believe that the Act should focus instead on establishing clear definitions of illegal content, and ensuring that platforms have the necessary policies, protocols, and systems in place to identify and remove violative content without delay.

A large percentage of complaints made to the DRCC may fall under Section 50(b), which deals with "an OCSP's decision to make content on its OCS inaccessible that the complainant believes does not meet the definition of harmful content." Because TikTok's Community Guidelines go well beyond the Proposal's definitions of harmful content, the adjudication of these complaints will often be moot. Indeed, the Proposal recognizes in Section 55 the right of an OCSP to "decide whether to make the content accessible or not, subject to their own guidelines." Having the DRCC review complaints where no relief can be provided to the complainant further raises questions about the utility of the body.

However, should the Government proceed with establishing the DRCC, we recommend providing OSCPs with an opportunity, upon receiving notice of a complaint under Section 50(b), to declare that the content was found to be violative of its own guidelines, separate from any analysis under the Act, and will not be restored on their platform. This will allow both the DRCC and OCSPs to avoid the unnecessary expenditure of resources on complaints where no relief can be provided. To further reduce frivolous and trivial complaints, or abuse of the appeal process, we also recommend that affected persons be required to initiate their own complaints through a portal maintained by the DRCC, rather than requiring the OCSP to initiate or transmit the complaint to the DRCC on the user's behalf. We support the requirement of Section 12(d) that once a user has exhausted an OCSP's appeals process, the OCSP's responsibility should be limited to providing notice of recourse available through the

THE MERICAN TECOMORONAMING ......

Tok

<sup>&</sup>lt;sup>8</sup> CyberTipline, National Center for Missing and Exploited Children. https://www.missingkids.org/gethelpnow/cybertipline

DRCC. Finally, in addition to the laudable commitments to diversity in the composition of the DRCC, we strongly recommend that the Act also take into consideration the importance of appointing members with relevant legal expertise, civil liberties experience, and industry experience in content moderation.

### Sections 67-68: Regulatory Charges

TikTok follows the laws of the countries where it operates, invests millions of dollars into platform safety, and has extensive and sophisticated content moderation practices in place. As already outlined, the scale and costs of the new regulatory bodies proposed are likely be enormous, with the DRCC alone potentially requiring thousands of content moderators to fulfill its mission.

To recover the costs of operating new regulatory bodies, the Proposal provides the government with discretion to assess regulatory charges to "one or more classes" of OCSPs. Potentially requiring only larger, established OCSPs such as TikTok to fund the new regulators could create significant inequities, with law abiding platforms paying the costs of policing nefarious platforms that flaunt Canada's jurisdiction. Those platforms, imageboards, and forums that operate outside Canada's laws are often the sources of harmful content, and will likely comprise the bulk of substantive complaints dealt with by the regulators. These services are unlikely to subject themselves to Canadian law or to pay regulatory charges. The Act must clearly define the criteria for classifying different classes of OCSPs, and if OCSPs are expected to pay regulatory charges, ensure that the charges are apportioned in a reasonable and proportionate way among *all* OCSPs that are accessible to persons in Canada.

### Conclusion

We agree with and support the main principles underlying the Proposal: a focus on systems and processes, a limited scope to defined categories of illegal content, and the use of transparency reporting to measure success. TikTok has invested in building a global, state-ofthe-art content moderation operation, and rather than the Government attempting to duplicate this capacity and expertise, it should work with platforms to ensure that moderation policies prohibit harmful content based on clear, actionable definitions provided in legislation, with workable timelines that incentivize accuracy over speed.

This legislation has the potential to be both effective and future proofed, while escaping the pitfalls of encouraging blanket over-moderation. We hope that the feedback we have provided is insightful and constructive towards ultimately developing a framework that will meaningfully reduce harmful content online while respecting the fundamental rights and freedoms of Canadians. We look forward to receiving further clarification on the feedback we have provided in this submission, and to working collaboratively with the Government towards our shared objective of combatting hate speech and other harmful content online. We would be pleased to answer any questions or provide additional information based on the feedback we have provided.

Sincerely,

Steve de Eyre Director, Public Policy & Government Affairs TikTok Canada

8

are commune at 10060200 harri

**cTok** 

Document communiqué en vertu de la Loi sur l'accès à l'information Document released pursuant to the Access to Information Act.

# Overhauling the Online Harms Proposal in Canada: A Human Rights Approach

Yuan Stevens & Vivek Krishnamurthy

September 2021



Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic
 Clinique d'Intérêt publique et de politique d'Internet du Canada Samuelson-Glushko



000157

Dissummit common phan in inmusio la (si) ann canada à Tullamiakan Distanomit infeasett dominant fo the Access in information (is)

# ABOUT CIPPIC

The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) is Canada's first and only public interest technology law clinic. Based at the Centre for Law, Technology and Society at the University of Ottawa's Faculty of Law, our team of legal experts and law students works together to advance the public interest on critical law and technology issues including privacy, free expression, intellectual property, telecommunications policy, and data and algorithmic governance.



The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic has licenced this work under a Creative Commons Attribution ShareAlike 4.0 International Licence.

Cover image art is provided by Mailchimp (2019)/Unsplash. Used under licence: https://unsplash.com/license.

The authors wish to thank Tamir Israel for his feedback and input on this submission.

# TABLE OF CONTENTS

INTRODUCTION: A NEW APPROACH IS NEEDED	7
THE DEFINITION OF SERVICE PROVIDERS IS IMPRECISE	2
Recommendations	4
THE 24-HOUR BLOCKING REQUIREMENTS MUST BE SCRAPPED	4
Recommendations	6
PROACTIVE CONTENT MONITORING AND FILTERING IS UNDEMOCRATIC	6
Recommendations	8
MANDATORY REPORTING TO LAW ENFORCEMENT MUST BE NARROWED	8
Recommendations	10
CONCLUSION	11

#### 000160

# INTRODUCTION: A NEW APPROACH IS NEEDED

Canada has long been a champion of human rights, democratic values, and internet freedom.<sup>1</sup> Canada co-founded the Media Freedom Coalition, which advocates for media freedom online and offline,<sup>2</sup> and next year Canada will chair the Freedom Online Coalition.<sup>3</sup> Canadians pride themselves on supporting internet freedom, protecting free expression, and serving as a leader in the protection of the freedom of association and assembly online worldwide.<sup>4</sup>

In this context, the government's proposed legislation to regulate online harms seriously undermines claims that Canada is a leader in human rights. By raising the spectre of content filtering and website blocking, the current proposal threatens fundamental freedoms and the survival of a free and open internet in Canada and beyond. In an effort to combat hate speech and other ills, the proposed law threatens the free expression and privacy rights of the very equality-seeking communities that it seeks to protect.

The online harms proposal combines some of the worst elements of other laws around the world.<sup>5</sup> This is why CIPPIC believes that the Department of Canadian Heritage needs to overhaul its current approach to addressing the problems caused by unlawful online content. We are seriously concerned about numerous elements of the proposed law — such as the lack of adequate transparency requirements, the loosened requirements for the Canadian Security Intelligence Service (CSIS) to obtain basic subscriber information, the various jurisdictional issues raised by the law, and whether an administrative body like the Digital Recourse Council should be able to determine what speech is legal under Canadian law.

The feedback we provide is focused on other key areas of concern. First, we focus on the need for increased clarity regarding which services or platforms are covered by the law. Second, we explain why the proposed 24-hour blocking requirement needs to be scrapped. Third, we demonstrate why the proposed proactive monitoring requirements need to be reined in. Finally, we advocate against the general requirement to identify and funnel

la Lai sui Docurrent the Access

<sup>&</sup>lt;sup>1</sup> "Reports on United Nations human rights treaties" (23 December 2020), *Government of Canada*, online: https://www.canada.canadan.heme.canadan.nitod-nations-system/reports-united-nationsfreeties.html.

<sup>&</sup>lt;sup>2</sup> "Media Freedom Coalition ministerial communiqué" (14 December 2020), *Government of Canada*, online: https://www.canada.ca/en/uloual-al/ans/camas/2020/11/media-in-adom-coalition-inmisterial-communique.html.

<sup>&</sup>lt;sup>3</sup> "Freedom Online Coalition", Freedom Online Coalition, online: https://weedomoni.weocolition.com.

<sup>&</sup>lt;sup>4</sup> "Internet freedom" (5 November 2020), *Government of Canada*, online: The state of the state

<sup>&</sup>lt;sup>5</sup> "Have your say: The Government's proposed approach to address harmful content online" (29 July 2021), *Government of Canada: Canadian Heritage*, online: <u>https://www.canada.ca/en/canadage</u>

<sup>;</sup> Michael Geist, "Picking Up Where Bill C-10 Left Off: The Canadian Government's Non-Consultation on Online Harms Legislation" (30 July 2021), *Michael Geist (blog)*, online: ; Daphne Keller, "Five Big Problems with Canada's Proposed Regulatory Framework for 'Harmful Online Content'" (31 August 2021), *Tech Policy Press*, online:



profiling information to law enforcement about people's online activity, in view of the chilling effects this will have on people's online behaviour.<sup>6</sup>

Canada is well-positioned to maintain its role as a global human rights leader and advocate for maintaining an internet that is open and free to all. A first step to preserving our role as a leader in this space involves an overhaul of this proposed law so that it is consistent with our democratic values.

# THE DEFINITION OF SERVICE PROVIDERS IS IMPRECISE

The proposal's definition of "online communication services" (OCSs) and "online communication service providers" (OCSPs) are imprecise and ill-suited to respond to the challenges posed by various kinds of unlawful online content.

Other countries have followed one of two options in defining to whom similar laws apply. Some countries' legislation goes broad and defines applicable services in a technologically neutral way, as has been done in Germany,<sup>7</sup> the EU,<sup>8</sup> and the US.<sup>9</sup> This approach involves crafting definitions that are malleable given technical developments. Others limit the scope to defined categories of service providers, as has been done in the UK<sup>10</sup> and Australia.<sup>11</sup> This approach involves setting out a taxonomy of services in light of the purposes they serve.

The government's proposal follows neither of these two dominant approaches. This is a problem as it renders the proposal's definitions of OCSs and OCSPs impermissibly vague. OCSs are defined as services accessible in Canada that have the "primary purpose" of allowing users of the service to "communicate with other users of the service, over the internet."<sup>12</sup> OCSPs are defined as "person[s] who provides an OCS."<sup>13</sup> With these definitions

<sup>&</sup>lt;sup>6</sup> Jon Penney, "Chilling Effects: Online Surveillance and Wikipedia Use" (2016) 31:1 Berkeley Tech LJ 117, online: https://oaoers.ssio.com/sol3/peoers.ntm?abstract\_rl=2709645.

<sup>&</sup>lt;sup>7</sup> Act to Improve Enforcement of the Law in Social Networks, 12 July 2017, § 2, 3 (2017) [NetzDG].

<sup>&</sup>lt;sup>8</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [Directive on E-Commerce], at art. 1(2); Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [Digital Services Act], at art. 1(1)(b).

<sup>&</sup>lt;sup>9</sup> *Title 47 U.S. Code* §*230* – Protection for private blocking and screening of offensive material [Section 230]; *Digital Millennium Copyright Act*, Public Law 105-304, Oct. 28, 1998 [DMCA], at s. 512(k)(1)(A).

<sup>&</sup>lt;sup>10</sup> Draft Online Safety Bill, (May 2021), online: https://www.pow.doc.event.euclided.com/com/online/safety-[] [Draft Online Safety Bill], at ss. 2 and 3.

<sup>&</sup>lt;sup>11</sup> Online Safety Act: An Act relating to online safety for Australians, and for other purposes, No. 76, 2021, online: https://www.lecis.auor.gov.au/Dataseccov.au/Datase

<sup>&</sup>lt;sup>12</sup> "Technical paper" (29 July 2021), Government of Canada: Canadian Heritage, online:

<sup>2.</sup> Excluded from this definition are services that "enable persons to engage only in private communications."

<sup>&</sup>lt;sup>13</sup> Ibid at para 4. The term "person" here presumably captures legal persons such as corporations. OCSPs exclude telecommunications service providers defined in the *Telecommunications Act*. OCSPs also exclude a person who indicates the "existence or location of content or hosts or caches the content or information about the location of the content, by reason only that another person who uses their services to provide an OCS."

la Lav sin Dolumen the Access to

a huge swath of the internet could qualify as an OCSP — including forum-based websites, dating platforms, blogs or news outlets with comment sections, and much more.

Canadian Heritage (PCH) officials attempted to clarify the meaning of these terms at an invite-only presentation delivered shortly after the announcement of the present consultation process.<sup>14</sup> According to the officials, the definition of OCSPs under the proposal would include social media platforms such as Facebook, Youtube, TikTok, Instagram, Twitter, as well as the website PornHub. Private communications and

Module 1 framewo	rk for	social	medi	ία	d reg	ulatory
Legislation w Providers (OC		soly to 't	Dnime C	ommu	niciatio	o Service
OCSPs:	Ð	⊡	F	0	Ø	Р.Н
Exempliary )	lar prive	ito com	munical	ION'S KIN	d (a)ec	ommunicalians
Excluded:	0	THUS	Bell	0	$\odot$	
Legislation w OCSPs	/süld n	ed capitoliv	la prod	velsar	d serve	sex that am not
Not OCSPs:	ø	x	0	00	e e	

from Canadian Hentage officials

telecommunications service providers that would be exempt include Shaw, Telus, Bell, WhatsApp, and Facebook Messenger. The slide deck also describes how the definition of OCSPs would not capture the fitness streaming app Peloton, an app for tracking diet and exercise called MyFitnessPal, the rideshare app Uber, and travel review site TripAdvisor.

The views stated at the briefing may reflect the government's intent, but this is not reflected in the definition of the terms OCS and OCSP in the technical paper.<sup>15</sup> Take TripAdvisor as an example — a site which features user-generated reviews of hotels and restaurants. According to PCH officials, the proposed legislation would not apply to TripAdvisor because it is not an OCSP. Yet TripAdvisor's core functionality involves hosting user-generated reviews of travel businesses that everyone on the internet can read, and registered users can upvote and flag. This core functionality is similar in many ways to YouTube, except YouTube hosts videos, while TripAdvisor hosts travel reviews. If YouTube meets the definition of a service available in Canada that has the "primary purpose" of allowing users of the service to "communicate with other users of the service, over the internet," then so too does TripAdvisor.

Correspondingly, the definitions of OCSs and OCSPs need to be refined to reflect what the government means for them to say.

There is a further problem with the proposed definitions of OCSs and OCSPs, which is that they are not up to the task of dealing with the serious problem of non-consensual distribution of intimate images (NCDII) over the internet. While the proposed legislation would clearly apply to a site like PornHub, the legislation does nothing to address the problem of NCDII on the vast array of websites and online services that have been created

 <sup>&</sup>lt;sup>14</sup> "Technical Discussion Paper: Online Harms Legislation", (August 2021) *Minister of Canadian Heritage, Minister of Public Safety and Emergency Preparedness, and Minister of Justice and the Attorney General.* <sup>15</sup> Indeed, it is inconsistent with rule of law principles for the public to have to rely on a slide deck distributed prior to an invite-only presentation to clarify the meaning of these terms.

4

to host such content, yet do not meet the statutory definition of an OCSP.<sup>16</sup> These difficulties point to the limitations of a "one size fits all" approach to addressing different kinds of online harms.<sup>17</sup>

# Recommendations

- The statutory language needs to precisely define which service providers this law applies to, and which it does not.
- Canada should follow international best practices and scope the legislation either in a broad and technologically neutral fashion, or narrowly so that it applies to a small range of specified services. Exceptions such as services that facilitate private communication should be equally as clear.<sup>18</sup>

# THE 24-HOUR BLOCKING REQUIREMENTS MUST BE SCRAPPED

The proposal's requirement that OCSPs block unlawful content within 24 hours of being notified that such content is available on their services should be scrapped, in view of the serious free expression concerns it raises. The proposed requirement is more heavy-handed even than Germany's controversial NetzDG law, given that the latter's 24-hour blocking requirement applies only to "manifestly" unlawful content.<sup>19</sup> NetzDG has served as a prototype for online censorship by authoritarian regimes around the globe,<sup>20</sup> and Canada

<sup>&</sup>lt;sup>17</sup> Cynthia Khoo, "Deplatforming Misogyny" (2021) Women's *Legal Action Fund*, online: ; Michael Geist, "'They Just Seemed Not to Listen to Any of Us' – Cynthia Khoo on the Canadian Government's Online Harms Consultation" (23 August 2021), *Law Bytes Podcast*, online:

<sup>&</sup>lt;sup>18</sup> When it comes to private communications specifically, any definition provided must be crafted in a way that does not compromise or undermine encryption technology, which is used to ensure the security and privacy of communication and serves numerous other purposes in society. See Lex Gill, Tamir Israel, and Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide" (14 May 2018) *Citizen Lab at the Munk School of Global Affairs & Public Policy*, online:

<sup>&</sup>lt;sup>19</sup> See e.g., Keller, *supra* note 5; "Germany: Flawed Social Media Law" (14 February 2018), *Human Rights Watch*, online: https://www.brw.org/news/2018/02/14/germany-llawed-social-media-law; "Eduction media-Comman Netz DO dram threatens freedom of expression" (23 May 2017), *EDRi*, online: https://doi.org/nutro.

<sup>&</sup>lt;sup>20</sup> Jacob Mchangama and Joelle Fiss, "The Digital Berlin Wall: How Germany (Accidentally) Created a Proto-type for Global Online Censorship" (16 November 2019), Global Freedom of Expression, Columbia University, online: https://dobal.centor.columbia.edu/publications/the-dobal-cento



places its long history of leadership in advocating for human rights at risk by following such an approach.

The proposal's draconian requirements are in sharp contrast to the immunity provided to service providers in the US for user-generated content,<sup>21</sup> and the requirement for "expeditious" removal of unlawful content in the UK<sup>22</sup> and the EU.<sup>23</sup> They may also be inconsistent with Canada's international obligations under Article 19.17 of the Canada-US-Mexico Agreement (CUSMA).<sup>24</sup>

Content moderation decisions are extremely difficult.<sup>25</sup> An enormous amount of content is uploaded daily to social media platforms, and the volume keeps growing as social media use increases.<sup>26</sup> Given the risk of massive fines of up to 5 percent of gross global revenues or \$25 million, online service providers are likely to remove vast quantities of lawful content to avoid the risk of liability under the proposed legislation.<sup>27</sup>

Simply put, Canada's proposed 24-hour blocking requirement will lead to over-removal and censorship of legitimate expression.<sup>28</sup> This in turn will have deleterious effects on the rights of marginalized communities to speak online — as evidence shows that such content is erroneously removed by online platforms much more frequently than content from mainstream groups.<sup>29</sup> Automated decision-making systems used to detect hate speech and harmful content are also particularly known to be biased against the posts of marginalized communities, such as Black and other racialized people.<sup>30</sup>

<sup>25</sup> Consider the takedown of the photo featuring the 'Napalm girl', which indicates that a balance must be found in moderation decisions between rights such as privacy and free expression. See Carmichael and Emily Laidlaw, "The Federat Government's Process to Address Comme Harris Explanation and Communa" (13 September 2021), *ABlawg.ca*.

<sup>26</sup> "Social Media Fact Sheet" (7 April 2021), Pew Research Center, online:

Cybersecure Policy Exchange, online: https://www.eybersecurepolicy.polic

28 Daphne Keller, supra note 19.

<sup>29</sup> See e.g., Kendra Albert et al, "FOSTA in a Legal Context" (2021) 52:3 *Columbia Human Rights LR* 1084, online: An and the standards in Social Media Content Moderation" (4 August 2021), *The Brennan Center*, online:

https://haconversation.com/usyond-a-technical-bug blased-atoc/thms-and-moderation-are-cereoringactivists-on-social-mode-15050; Shirin Ghaffary, "The algorithms that detect hate speech online are biased

<sup>&</sup>lt;sup>21</sup> "Section 230 of the Communications Decency Act", *Electronic Frontier Foundation*, online: https://www.eh.org/issues/cde230.

<sup>&</sup>lt;sup>22</sup> Draft Online Safety Bill, supra note 10 at. s. 9(3)(d).

<sup>&</sup>lt;sup>23</sup> Directive on E-Commerce, *supra* note 8, at arts. 13 and 14; Digital Services Act, *supra* note 8, at arts. 4 and 5.

<sup>&</sup>lt;sup>24</sup> Vivek Krishnamurthy and Jessica Fjeld, "CDA 230 Goes North American? Examining the Impacts of the USMCA's Intermediary Liability Provisions in Canada and the United States" (July 2020), *Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) and the Harvard Law School's Cyberlaw Clinic*, online:

Harms Disinformation and Online Harms on Private Messaging Platforms in Canada" (11 May 2021),

<sup>&</sup>lt;sup>27</sup> Technical paper, *supra* note 12 at para 119.

In ost //www.chrunenioniter.crg/on-work/nates chi-reports/double-standurds social-media-contentmoderations

<sup>&</sup>lt;sup>30</sup> See e.g., Merlyna Lim and Ghadah Alrasheed, "Beyond a technical bug: Biased algorithms and moderation are censoring activists on social media" (16 May 2021), *The Conversation*, online:

Whether private corporations should be responsible for striking the delicate balance between safety, privacy, and freedom of expression is worth scrutinizing.<sup>31</sup> To the extent that a government is privatizing this function by requiring platforms to determine whether content on their sites is illegal, the government should provide platforms with incentives to do so in a transparent and fair-minded fashion.<sup>32</sup> Unfortunately, the government's proposal fails in these regards.

Safeguards are needed that protect freedom of expression for all content removal decisions, including the ability to contest the removal of material. If the government wishes to require OCSPs to remove illegal content, a better alternative is to require them to do so expeditiously rather than setting a precise 24-hour limit.

## Recommendations

The 24-hour blocking requirement should be scrapped.

If service providers are required to assess and block illegal content, a better approach is to provide for a general requirement to do so expeditiously.

# PROACTIVE CONTENT MONITORING AND FILTERING IS UNDEMOCRATIC

CIPPIC views the proposed legislation's proactive monitoring and filtering requirements as fundamentally flawed. By requiring OCSPs to proactively monitor and filter content online, the Canadian government risks conscripting the private sector to engage in a form of dragnet surveillance that would have a chilling effect on people's communications and behaviour online, and pose risks to their privacy. Such a requirement has no place in Canadian legislation, especially in tandem with mandatory reporting to law enforcement.

The proposal requires OCSPs to take all reasonable measures, including through use of automated systems, to identify harmful content and make it inaccessible to people in Canada.<sup>33</sup> OCSPs could also be ordered by the proposed Digital Safety Commissioner to do

6

la Ln) sui Documern the Arces

against black people" (15 August 2019), Vox, online: https://www.com/ecoder/2019/5/15/2020638//subalroadic-hale-an-each-dac-black an encoder-facebland-faceblack

<sup>&</sup>lt;sup>31</sup> Jillian C. York, *Silicon Values: The Future of Free Speech Under Surveillance Capitalism*, (Brooklyn, NY: Verso Books, 2021); Kirsten Gollatz, Martin J. Riedl, and Jens Pohlmann, "Removals of online hate speech in numbers" (9 August 2018), *Alexander von Humboldt Institute for Internet and Society (HIIG)*, online:

<sup>&</sup>lt;sup>32</sup> The Canadian government's proposal also falls short of the public reporting requirements set out in the NetzDG for platforms that receive more than 100 complaints per year, which was one of the few parts of the law that received the most universal support. Heidi Tworek and Paddy Leerssen, "An Analysis of Germany's NetzDG Law" (15 April 2019), *Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression*, online:

<sup>&</sup>lt;sup>33</sup> Technical paper, *supra* note 12 at para 10.

"any act or thing necessary" to ensure compliance under the proposed law, including proactive monitoring.<sup>34</sup>

Requirements to proactively monitor and filter online content are tantamount to prepublication censorship.<sup>35</sup> From a legal standpoint, obligating OCSPs to take all reasonable measures to identify content falling within the proposals' harm categories can effectively amount to a general monitoring obligation. While the technical paper indicates that nothing in the proposal would require or authorize an OCSP to seek out content falling outside the Act's five harm categories, in practice proactively discovering *any* harmful content requires monitoring *all* content.<sup>36</sup> General monitoring obligations are inherently intrusive and deeply disproportionate.

The legal requirement to proactively discover harmful content also violates Canada's trade obligations. Article 19.17 of the Canada-United States-Mexico Agreement (CUSMA) prohibits Canada from imposing liability on a platform as if it was the originator of illegal content.<sup>37</sup> Under the government's proposal, however, platforms will face steep penalties if they fail to proactively remove harmful content, in accordance with regulatory orders issued to secure compliance with the proposed Act's content identification and proactive removal obligations.<sup>38</sup> By making platforms directly responsible for assessing the legality of all user-generated content, the proposal treats platforms identically to content creators in violation of CUSMA.<sup>39</sup>

<sup>39</sup> CUSMA, *supra* note 24. We note that paragraph 4(c)(i) of Article 19.17 exempts measures taken to enforce criminal law. However, the online harm categories adopted in the proposal explicitly extend beyond criminally prohibited content (Technical Paper, *supra* note 12 at para 8).

For example, in outlining the parameters of child exploitation material, the proposal indicates that: "The concept ... should capture ... material ... that may not constitute a criminal offence...". Similarly, the proposal does not rely on the Criminal Code definition of hate speech, but rather the broader regulatory definition which the Government intends to introduce in parallel amendments to the *Canadian Human Rights Act*. This definition modelled on the Supreme Court of Canada's guidance regarding the appropriate scope of regulation for hate speech in.a regulatory context, which is explicitly broader than the Criminal Code definition (see e.g., *Saskatchewan (Human Rights Commission) v Whatcott*, 2013 SCC 11, at para 105.

Beyond this explicit extension in the hate speech context, none of the content definitions adopted in the proposal include a mens rea requirement in their definition. For example, the proposed definition for nonconsensually distributed intimate images encompasses content where "it is not possible to assess if a consent to the distribution was given by the person depicted in the image or video." While this definition is defensible in a regulatory context (see e.g., Emily Laidlaw et al, "Nonconsensual Disclosure of Intimate Images (NCDII) Tort" (August 2019), *Uniform Law Conference of Canada*), online: **Content of the Content of the Criminal Code**, RSC 1985, c C-46. Correspondingly, this cannot fall within the exception in paragraph 4(c)(i) of Article 19.17. The proposal would additionally empower the government to define specific harmful content 'terms' through an Order-in-Council (Technical Paper, para 9).

la LTI sui Docurent the Arces

<sup>&</sup>lt;sup>34</sup> Ibid at para 80.

<sup>&</sup>lt;sup>35</sup> Carmichael and Laidlaw, *supra* note 24. The duty of care model may indeed be interpreted as enabling a proactive monitoring requirement in those countries.

<sup>&</sup>lt;sup>36</sup> Ibid at para 9.

<sup>&</sup>lt;sup>37</sup> Canada-United States-Mexico Agreement, 30 November 2018, online: https://www.merice.org/add/ commence.org/add//discourse-commence.org/add//discourse-commence.org/add//discourse-commence.org/add//discourse-

<sup>19.17;</sup> Krishnamurthy and Fjeld, supra note 24.

<sup>&</sup>lt;sup>38</sup> Technical paper, *supra* note 12 at paras 10, 80 and 94(a).

the Access to

10 [ 71) 81

8

The proactive monitoring requirement must also be considered in light of the proposed provisions requiring mandatory reporting of unlawful content to law enforcement. These monitoring and filtering requirements will have discriminatory impacts on marginalized and racialized communities, who already face barriers to engaging in the public sphere online.<sup>40</sup> The combination of these requirements is draconian and will further exacerbate the overpolicing and surveillance of racialized communities online.

The government's proposal would make Canada an outlier in comparison to its global peers. There is no general obligation to monitor online content in Germany, the EU, and the US,<sup>41</sup> while Australia and the UK use a duty of care model.<sup>42</sup> Actual knowledge is required for any monitoring (and reporting) of child sexual exploitation material in the US<sup>43</sup> and for intermediary liability to attach in the EU.<sup>44</sup>

# Recommendations

- There should be no general requirement to proactively monitor content, including across all types of regulated content.
- While the law need not prohibit voluntary proactive monitoring initiatives already in place, it must be explicit that it does not impose or authorize any legally binding proactive monitoring obligations at all.

# MANDATORY REPORTING TO LAW ENFORCEMENT MUST BE NARROWED

CIPPIC has serious concerns about the government's proposed requirement that OCSPs report certain kinds of content to the RCMP and CSIS. Such mandatory reporting requirements, when combined with the proactive monitoring requirements detailed above, pose an unacceptable risk to the privacy rights of Canadians. Such measures should have no place in the laws of a free and democratic society. In any case, there needs to be actual

There is no obligation that the resulting definitions will respect baseline mens rea knowledge requirements inherent in the government's criminal law power.

Finally, we note that paragraph 4(c)(ii) of Article 19.17 of CUSMA also exempts "specific, lawful order(s) of a law enforcement authority" from the scope of its intermediary liability protections. However, compliance orders realizing a platform's general obligation to discover and remove all content falling within the proposal's harm categories are not 'specific' and, moreover, are inconsistent with Article 19.17 more broadly (see footnote 8 to that Article).

<sup>&</sup>lt;sup>40</sup> Carmichael and Laidlaw, supra note 24; Khoo, supra note 17 at 200.

<sup>&</sup>lt;sup>41</sup> NetzDG, supra note 7; E-Commerce Directive, supra note 8, at art. 15; Section 230, supra note 9.

<sup>&</sup>lt;sup>42</sup> Online Safety Act, *supra* note 11; Draft Online Safety Bill, *supra* note 10. See also Carmichael and Laidlaw, *supra* note 24, who note that the duty of care model may indeed be interpreted as enabling a proactive monitoring requirement in those countries.

<sup>&</sup>lt;sup>43</sup> 18 U.S. Code § 2258A – Reporting requirements of providers.

<sup>&</sup>lt;sup>44</sup> E-Commerce Directive, supra note 8, at arts. 12-15.



9

knowledge of wrongdoing before service providers are required to notify law enforcement of illegal conduct.

The technical paper proposes significant changes to the current mandatory reporting regime for online service providers, which applies only to child sexual abuse material that a service provider discovers in the course of its operations. Part E of the government's proposal would require OCSPs to do one of the following:

- Approach A: Notify the RCMP when it has reasonable grounds to suspect that content falling within the 5 categories of regulated harmful content reflects an imminent risk of serious harm to any person or to property;<sup>45</sup>
- Approach B: Report "prescribed information" in respect of "prescribed criminal offences" within the 5 categories of regulated harmful content to "prescribed" law enforcement officers or agencies.<sup>46</sup>

For Approach B, OCSPs would be required to report information to CSIS about terrorist content and content that incites violence — both of which are subject to the proposal's 24-hour removal requirement.<sup>47</sup> This approach would also require OCSPs to report to CSIS in secret if the disclosure "could be injurious to national security."<sup>48</sup> Under both approaches, the government will have the option of obligating OCSPs to include identification information— including the names and account identifiers of anyone implicated in the report.<sup>49</sup> Module 2 of the proposal would impose a similar customer identification obligation on ISPs such as Bell and TELUS with respect to child exploitation material.

The government's proposals are unprecedented among democratic nations. The only approach to mandatory reporting that resembles what is being proposed here are amendments to Germany's NetzDG in 2020, which requires service providers to report certain types of criminal content to federal law enforcement even before suspicion has been established.<sup>50</sup> The reporting requirements under the German law have been characterized as allowing "user data to be passed to law enforcement before it is clear any crime has been committed," and their constitutionality is being challenged in the German courts.<sup>51</sup> Yet Canada's proposal is even more extreme than the German proposal, in that the government will be empowered to force provision of identification information such as customer names and addresses.

<sup>50</sup> Phillip Grüll, "German online hate speech reform criticised for allowing 'backdoor' data collection" (19 June 2020), *Euractiv*, online:

<sup>51</sup> "Google takes legal action over Germany's expanded hate-speech law" (27 July 2021), *Reuters*, online:

<sup>&</sup>lt;sup>45</sup> Technical paper, *supra* note 12 at para 20.

<sup>46</sup> Ibid.

<sup>47</sup> Ibid at para 22.

<sup>48</sup> Ibid at para 27.

<sup>&</sup>lt;sup>49</sup> Technical paper, *supra* note 12 at para 32. While the government must take into account "the privacy interests engaged" by any information it mandates for disclosure, other elements of the Technical paper confirm that the government currently considers subscriber identification information to be fair game (see e.g., Module 2 of the Technical paper at para 8).



10 171.81

the Access

The government's sweeping proposal far exceeds what is being considered in Australia and the United Kingdom. Proposals in those countries would obligate online harms regulators to report and disclose certain user activity to law enforcement if discovered during the course of their regulatory oversight activities.<sup>52</sup> Neither appears to contemplate an open-ended obligation to monitor all user content and report any user suspected of violating one of the Proposal's harm categories to law enforcement or national security bodies. Similarly, reporting obligations currently imposed on service providers in the United States and on Canadian ISPs are limited to child exploitation material and, more importantly, do not include any open-ended content discoverability mandate.<sup>53</sup> An EU proposal is similarly limited, in that it would only require service providers to report instances where the platform discovers a serious crime that poses a threat to life but imposes no proactive monitoring requirement.<sup>54</sup>

While each of these proposals poses its own challenges and problems, the combination of proactive discovery and reporting obligations in the proposal effectively transforms Canada's service providers into an investigative tool for law enforcement and CSIS. This is especially so given that the identification and classification — and even reporting — processes are likely to be automated given the volume of content at issue.

Online service providers in Canada must not be turned into "suspicion databases."<sup>55</sup> As Carmichael and Laidlaw observe, some major service providers already engage in the first of the proposal's approaches on a voluntary basis.<sup>56</sup> The second approach laid out in the consultation paper is particularly worrying because it may capture a wide range of content and activity that is legal. By requiring platforms to feed data on their users to the RCMP and CSIS, the epidemic of surveillance and over-policing faced by marginalized and equality-seeking groups in Canada in the offline sphere will be extended online as well.<sup>57</sup>

# Recommendations

- Reporting obligations should remain limited to child exploitation material.
- Reporting requirements must remain limited to content that service providers discover through the general course of providing their services. A reporting obligation cannot be combined with a proactive content discovery obligation.

<sup>56</sup> Carmichael and Laidlaw, supra note 19.

<sup>&</sup>lt;sup>52</sup> Online Safety Act, *supra* note 11 at s. 224; "Online Safety Bill Impact Assessment" (26 April 2021), UK Department for Digital, Culture, Media and Sport, online:

Hilps, Vassel s, bublishing, service, goy Ak/goyernmen/Uplcads/svalet viubloads/ariabhmeni\_dois/Ele/M6283, Dr art: Online, Sylety, Bill - Impact, Assessment, Web, Accessible, odi at paras 205-206.

 <sup>&</sup>lt;sup>53</sup> United States, Sexual Exploitation and Other Abuse of Children, 18 USC 2258A; Canada, *Mandatory Reporting of Internet Child Pornography by Persons who Provide an Internet Service Act*, SC 2011, c 4, at s 2.
 <sup>54</sup> Digital Services Act, *supra* note 8 at recital 48.

Digital Services Act, supra note 8 at

<sup>&</sup>lt;sup>55</sup> Grüll, supra note 48.

<sup>&</sup>lt;sup>57</sup> Kate Robertson, Cynthia Khoo, and Yolanda Song, "To Surveil and Protect: A Human Rights Analysis of Algorithmic Policing in Canada" (1 September 2020) *Citizen Lab at the Munk School of Global Affairs & Public Policy*, online: at 3.

# CONCLUSION

CIPPIC believes that the proposed legislation is fundamentally flawed. As Parliament reconvenes after the recent election, we call upon the new government to reconsider Canada's approach to online regulation. Rather than focusing just on online harms, the government should tackle platform regulation holistically — as is happening in the European Union with the introduction of the Digital Services Act and the Digital Markets Act in tandem.<sup>58</sup>

Online harms also cannot be legislated in isolation. There is a growing consensus that platform amplification of harmful material is a symptom of business models premised on surveillance capitalism<sup>59</sup> and the concentration of market power by technology companies.<sup>60</sup>

Canada needs to reconsider its approach to platform regulation from the ground up. We urge the Government of Canada to engage in significant study and consultation with experts and stakeholders in Canada and beyond. A comprehensive regulatory strategy is needed that aligns with efforts in like-minded countries, and that respects the global nature of the internet.<sup>61</sup>

A new approach that prioritizes the respect of human rights and internet freedom is needed. And the first step of that approach must be to set aside this proposal. Anything less will jeopardize Canada's claim to being a leader in advancing free expression, a free and open internet, and the human rights upon which our democratic society has been built.

<sup>&</sup>lt;sup>58</sup> Digital Services act, *supra* note 8; "The Digital Markets Act: ensuring fair and open digital markets" (2019), *European Commission*, online:

<sup>&</sup>lt;sup>59</sup> See e.g., Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, (New York, NY: PublicAffairs, 2019); Jillian C. York, *supra* note 29.

<sup>&</sup>lt;sup>60</sup> Vas Bednar and Robin Shaban, "The State of Competition Policy in Canada: Towards an Agenda for Reform in a Digital Era" (21 April 2021), *Centre for Media, Technology and Democracy*, online:

https://www.media.condemocracy.com/work/the state of condectuon policy in cariada.

<sup>&</sup>lt;sup>61</sup> See e.g., Ron Deibert, *Reset: Reclaiming the Internet for Civil Society*, (Toronto: House of Anansi, 202) at pp. 15-16.

hanstanten er en sterktigte som konstant hver program som konstanten att som kanstanten för att som konstanten att som tille store stör som att som konstanten som

## Submission of Internet Archive Canada in Response to the Government's Proposed Approach to Address Harmful Content Online

September 24, 2021

## Submitted by: Lila Bailey, Policy Counsel, and Peter M. Routhier, Policy Fellow.

Internet Archive Canada is a not-for-profit digital library whose mission is to provide universal access to all knowledge. Over more than a decade of operations in Canada, Internet Archive Canada has digitized more than 650,000 books and other works, a great many of which are focused on specifically Canadian cultural heritage and historical government publications.<sup>1</sup> This work has been done with a dedicated staff of Canadians in partnership with more than 300 Canadian libraries and memory institutions (such as University of Toronto and Library and Archives Canada/ Bibliothèque et Archives Canada). Like a paper library, Internet Archive provides free access to much of these materials to researchers, historians, scholars, the print disabled, and the general public.<sup>2</sup>

While this proposal appears centered around large social media platforms, we have deep concerns about it, including its potential for broad application to libraries and small and not-for-profit organizations like ours. We believe that libraries and others like us have a role to play in creating and sustaining a better internet, with more digital public spaces and more access to good and trustworthy information online.<sup>3</sup> Unfortunately, imposing newly burdensome and potentially overbroad regulatory regimes—even with the best of intentions—is likely to make the costs of participation in certain digital spaces too high for all but the largest commercial actors. The result will be further entrenchment of the largest foreign corporations in positions of dominance online.<sup>4</sup> Should the government proceed with this proposal, it should carefully consider the extent to which it will make it even more difficult for truly Canadian spaces to survive and thrive online, leaving us with a worse information ecosystem overall.

## 1. Digital Public Spaces

As we understand it, the government's proposal would impose substantial costs, financial and otherwise, on any entity which is deemed to fall within the definition of an Online Communication Service. The definition could change by regulation at any time. This would make it a risky proposition to participate in online life in any way close to the definition of an OCS; with a change in definition, or even in interpretation, substantial

<sup>&</sup>lt;sup>1</sup> https://archive.org/details/toronto

<sup>&</sup>lt;sup>2</sup> Internet Archive Canada works with the Internet Archive (also a not-for-profit organization) to make these materials accessible to the general public in Canada and throughout the world.

<sup>&</sup>lt;sup>3</sup> See, e.g., https://publicspaces.net/; https://culturalfoundation.eu/programmes/digitaleuropean-public-spaces/; https://www.eff.org/deeplinks/2021/05/introducing-public-interestinternet.

<sup>&</sup>lt;sup>4</sup> See https://www.politico.eu/article/europe-data-protection-gdpr- general-data- protectionregulation-facebook-google/

investments of time, energy, and other resources could evaporate. And for those clearly within the concept of an OCS—whatever that is deemed to be—the costs of automated systems, the technical and human resources required to implement twenty-four hour takedowns, and all the actual and possible associated requirements, would be extraordinarily high. How could these be met by small libraries, not-for-profits, or startups? How could any but the largest multinational corporations play a part in shaping the online world? Would that situation truly address the problems at hand?

It is also important to consider the broader global context. If new and different rules are to be adopted in jurisdictions around the world, the costs of complying with each of them will multiply. This is, one must assume, why provisions like Article 19.17 of the CUSMA have been proposed and agreed to by Canada and many others. Will others ignore treaty obligations and promulgate conflicting rules? Will Canada's adoption of unique, costly, and open-ended regulations—with potential application to broad swaths of actors and online speech—improve Canada's internet, or make it a hinterland?

## 2. The Information Ecosystem

Libraries have long been a cornerstone of a free and open society; indeed, "One of the Canadian Library Association's core beliefs is that the principles of intellectual freedom and unfettered universal access to information, through libraries, are key components of an open and democratic society."<sup>5</sup> We worry deeply about the effect this proposal could have on libraries and our information ecosystem overall.

Libraries must be able to play our traditional role in digital spaces, today and in the future, or we risk losing a cornerstone of our free and open society. More narrowly, we risk losing a corrective to disinformation and misinformation online. What effect will the threat of severe financial penalties, to say nothing of compliance costs, have on the development and maintenance of library collections online? What effect will this proposal have on our information ecosystem more broadly? This proposal—appearing, as far as we can tell, after private government discussions with big tech companies and others, but not with libraries like us—does not appear to have considered it.

## 3. Conclusion

Even laws put forward with the best of intentions, and directed in concept to the worst of the worst, can have dangerous consequences.<sup>6</sup> If this proposal is not rejected outright, the government should take a step back, and engage in a thorough and truly open process of consideration and review, before taking drastic action.

<sup>&</sup>lt;sup>5</sup> https://blogs.ifla.org/school-libraries/2016/02/28/canada-intellectual-freedom-award-to-teacher-librarians/

<sup>&</sup>lt;sup>6</sup> https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filteringblocking-and-reporting-rules-1

25 September 2021

To Whom It May Concern:

My comments address the technical paper that will inform the government's approach to online harms. The technical paper proposes to:

- 1. establish new information sharing between police, security agencies, and OSCs as well as create new obligations for TSPs;
- 2. mitigate five distinct categories of criminal activity or online harms; and,
- 3. propose a new regulatory framework for the oversight of commercial content moderation online.

These three objectives, debatable in their own rights, invoke distinct policy traditions and fields of expertise. I am concerned that the technical paper conflates these three separate issues into one legislative agenda.

My submission focuses on the third objective, the new regulatory framework. Before focusing on the third objective, I note:

1. Changes to the administration of the criminal code for OCSs must be treated separately from the regulatory framework for content moderation

At present, the technical paper too often frames online harms as a policing problem at a time when the biases and oversight of Canada's policing services are evident and calls for reforms clear and needed. The distinction between online harms and criminal activities remains ambiguous in the technical paper. Conflating harm and criminal acts risks deputizing OSCPs with both enforcement and police reporting for criminal activities.<sup>1</sup> Proposal 20 specifically requires a separate consultation phase and it should not be assumed that because automated content takedowns are happening that automated content takedowns are an effective or central instrument to address online harms. Furthermore, the technical paper's overall focus on OSC regulation is diluted

<sup>&</sup>lt;sup>1</sup> For a distinction, see: Tenove, Chris, Heidi Tworek, and Fenwick McKelvey. "Poisoning Democracy: How Canada Can Address Harmful Speech Online." Ottawa: Public Policy Forum, November 8, 2018. <u>https://www.ppforum.ca/wp-content/uploads/2018/11/PoisoningDemocracy-PPF-1.pdf</u>.

with its discussion of new measures for Internet services and new blocking/filtering obligations for Telecommunications Service Providers. These powers are out of scope and arguably within the power of the CRTC to implement if needed already.

## 2. Comparability of these five online harms is debatable and more targeted legislation may prove more effective

The five online harms need further definition. Furthermore, the nuances of each online harm, such as the national and international dimensions of terrorist activities, for example, may not be well suited for an omnibus framework.<sup>2</sup> Protecting Canada's democracy, ostensibly another online harm, has been addressed through reforms to Canada's Elections Act.

## 3. Online harms require a whole of society approach that is out of scope with aspects of this bill focused on OSCs

More accountability to commercial content moderation has not and will not resolve the root causes of online.<sup>3</sup> Rather, better regulation of already-existing content moderation is enough of a regulatory accomplishment without the added challenge of suggesting that content moderation as a first response to systemic injustice.

With these primary concerns in mind, I move to the administrative aspects. I acknowledge that content moderation is a needed part of inclusive communication systems, but certainly not more important than matters of access, affordability, and inclusion. As part of these the broader reforms to Canada's communication system, the technical paper that:

1. Defines the regulatory category of OSC in line with the CRTC's suggested reforms in CRTC 2017-359 for new domain/industry-specific media regulation categories distinct from a TSP.

<sup>2</sup> For a more detailed discussion of focused reforms, see: Khoo, Cynthia. "Deplatforming Misogyny," Technology-Facilitated Violence. Toronto: Women's Legal Education and Action Fund,

2021. <u>https://www.leaf.ca/publication/deplatforming-misogyny/</u>. <sup>3</sup> McKelvey, Fenwick. "Toward Contextualizing Not Just Containing Right-Wing Extremisms on Social Media: The Limits of Walled Strategies." *SSRC Items* (blog), July 13, 2021. https://items.ssrc.org/extremism-online/toward-contextualizing-not-just-containing-right-wing extremisms-on-social-media-the-limits-of-walled-strategies/.

- 2. Establishes a Digital Safety Commission that includes a Digital Resource Council of Canada, and an Advisory Board to monitor compliance and administer OSCPs enforcement of online harms;
- 3. Sets new obligations for OSCPs to report and filter 5 types of illegal content; and,
- Grants the DSC new powers including AMPs for OSCPs as well as inspection powers.

The regulatory framework seems a viable opportunity if primarily seen as a mechanism to enhance oversight and transparency for commercial content moderation<sup>4</sup> and algorithmic filtering.<sup>5</sup> The DSC's powers to investigate are welcome additions to Canada's media institutions especially since the DSC is subject to the Access to Information Act. As access to data is a primary barrier to research into OSCs,<sup>6</sup> the DSC may enhance public knowledge of largely opaque moderation practices.

The DSC's mandate must be defined with clear policy objectives. I recommend its policy objectives follow Dr. Suzie Dunn who suggests that, "Canada's approach to regulating platforms should centre human rights, substantive equality, and intersectionality, and employ a trauma-informed approach."<sup>7</sup>

I am expressly supportive of DSC's power to investigate how an OSCP monetizes harmful content (14f) and encourage more attention to this function in the subsequent act.

The technical paper, at present, does not provide a timeline for the constitution of the DSC. I recommend that:

- 1. Reporting and inspection powers be prioritized as a first step before automated takedown obligations come into effect;
- 2. The DSC establish a Technical Standards Committee with Measurement Canada, the CRTC, OSCPs, civil society, and academics to develop information gathering and potentially an equivalent of the CRTC Monitoring Report to establish a public

<sup>5</sup> Hunt, R., & McKelvey, F. (2019). Algorithmic Regulation in Media and Cultural Policy: A Framework to Evaluate Barriers to Accountability. *Journal of Information Policy*, *9*, 307–335. JSTOR. <u>https://doi.org/10.5325/jinfopoli.9.2019.0307</u> <sup>6</sup> Tromble, Rebekah. "Where Have All the Data Gone? A Critical Reflection on Academic Digital

<sup>&</sup>lt;sup>4</sup> Roberts, S. T. (2019). *Behind the screen: Content moderation in the shadows of social media.* Yale University Press.

<sup>&</sup>lt;sup>8</sup> Tromble, Rebekah. "Where Have All the Data Gone? A Critical Reflection on Academic Digital Research in the Post-API Age." *Social Media + Society* 7, no. 1 (January 1, 2021): 2056305121988929. <u>https://doi.org/10.1177/2056305121988929</u>; Tworek, Heidi. "Open Access to Data Is Critical in a Democracy." Centre for International Governance Innovation, August 25, 2021. https://www.cigionline.org/articles/coord-access to data is critical in a democracy."

https://www.cigionline.org/articles/open-access-to-data-is-critical-in-a-democracy/. <sup>7</sup> Dunn, Suzie, William Perrin, and Heidi Tworek. "What Can Canadian Law Makers Draw from the New UK Online Safety Bill?" Centre for International Governance Innovation, May 20, 2021. <u>https://www.cigionline.org/articles/what-can-canadian-law-makers-draw-new-uk-online-safet</u> <u>v-bill/</u>.

record about the threat of online harms and the state of commercial content moderation and automated content recommendation;

- 3. All matters of composition (46, 64, and 71) be changed from *considering* inclusive membership to *requiring* inclusive membership and establish better democratic oversight of candidate selection and vetting as proposed in the BTLR report;
- 4. Ensure sufficient budget and effective reporting mechanisms before implementing blocking and filtering regimes.

My timeline emphasizes focusing the DSC first on enhancing transparency first on commercial content moderation then secondly considering its effectiveness to combat online harms. Ideally, other measures or more dedicated initiatives could develop simultaneously taking a whole-of-society approach to the 5 identified online harms.

The present risk is that the 24-hr takedown requirement along with a lack of penalties for false positives may encourage OSCPs to further invest in automated content moderation, especially artificial intelligence as a form of media governance.

The consideration of automated content regulation is lacking in the current working paper and needs substantive consideration. The technical paper does not address its responsibility nor its legitimization of artificial intelligence as used by OSCPs to classify, filter, and demote harmful content. The technical paper proposed a regime legitimating automated content regulation at scale without sufficient records of the efficacy of the systems in Canada's both official languages and in Canada's multicultural society. The technical paper needs an substantively expanded discussion of AI accountability including times when the potential risks require the prohibition of automated solutions.<sup>8</sup>

The DSC may need powers to designate standards for content moderation work that then prohibit AI as high-risk applications and better accountability mechanisms. Inversely, outsourcing and ghost labour in commercial content moderation require better labour standards and safer working environments. At present, the labour of moderation is assumed to be automatable and without long-term harm to the workers.

The DSC must be seen as a promising beginning that must proceed cautiously to build knowledge, expertise, and autonomy before implementing content takedowns (11a) recognizing instead that better accountability to already-existing content moderation.

<sup>8</sup> Balayn, Agathe, and Seda Gürses. "Beyond Debiasing: Regulating AI and Its Inequalities." Brussels: European Digital Rights, 2021. https://edri.org/our-work/if-ai-is-the-problem-is-debiasing-the-solution/. reporting and oversight is a needed first step before assuming that content takedowns will be an adequate form of online harms that require a whole-of-society approach.

The technical paper and discussion papers mark an early first step that hopefully leads to a more fulsome consultation, public record, and clearer legislative agenda. I continue to support these efforts in my research and my opinion here.

Sincerely,

Fenwick McKelvey

kan tarbah esan tertapi sen senara lari tertapi da san si 6 Pullantakan 2005 apada akaran tertapi da si 10 Sucesti dentara tarbah si

24 September 2021

s.19(1)

Michele Austin

Ilvitier Cariada

CONFIDENTIAL

Department of Canadian Heritage 25 Eddy St Gatineau QC K1A 0S5 By email: pch.icn-dci.pch@canada.ca

RE: The Canadian government's proposed approach to address harmful content online

To Whom It May Concern:

On behalf of Twitter, thank you for the opportunity to respond to the Government of Canada's proposed approach to regulating online content.

Online safety is a shared responsibility. Digital service providers as well as governments, private citizens and network service providers play an important role in protecting their communities from harmful content online,

We create rules to keep people safe on Twitter and promote healthy conversations. Our rules are continuously evolving to reflect the realities of the conditions in which we operate.

Under our rules, Twitter currently takes action on all categories of content listed in this consultation (terrorist content; content that incites violence; hate; non consensual sharing of intimate images; and child sexual exploitation content). The five categories are also currently actionable under existing Canadian criminal and civil law. Each of the categories of content listed in this consultation is the subject of an offence under the *Criminal Code of Canada*. The *Criminal Code* prohibits publishing and distributing non-consensual sexual images<sup>1</sup> and child sexual exploitation<sup>2</sup>, promoting hate propaganda<sup>3</sup>, instructing or counselling a person to commit a terrorism offence<sup>4,</sup> and communicating statements that incite violence<sup>5</sup>. The *Mandatory Reporting Act* requires reporting of online child sexual exploitation<sup>6</sup>. The Canadian common and civil law regimes also provide recourse and remedies to those who have suffered harm from these kinds of activities.

Any changes proposed by this consultation should be mirrored by amendments to the *Criminal Code of Canada* and the *Mandatory Reporting Act*. Twitter would like to emphasize that online content regulation requires a proportionate approach to balance protections from harm, on one hand, against the fundamental right to freedom of expression under the *Canadian Charter of Rights and Freedoms* and against the right to procedural fairness and privacy, on the other. This is a fine balance, and requires a tailored and constantly evolving approach.

When the right balance is struck, companies and regulators alike have clearly delineated responsibilities regarding protections for users' rights, and a shared commitment to foster a diverse public conversation consistent with community expectations within a free and democratic society like Canada. We welcome the opportunity to comment on how to achieve that balance.

As we continue to develop and review Twitter's rules in response to changing behaviors and challenges with serving the public conversation, we understand the importance of considering a global perspective and thinking about how policies may impact different communities and cultures equally. Since 2019, we've prioritized feedback from the public, external experts, and our own teams to inform the continued development of our policies.

Further to our comments on the proposal, Twitter is calling for:

- Consideration of a much wider range of interventions to deliver online safety than proposed, such as renewed emphasis on media literacy and education; greater user control over and choice between algorithms; and the importance of open standards.
- Recognizing personal choice and affording the ability to do nothing. As the work of the Canadian Media Ecosystem Observatory<sup>7</sup> has illustrated with regard to political content, actioning some content can cause it to spread not just on its own terms, but through other channels such as traditional media in their coverage of the actioned content. Once this content is amplified "out in the wild" it can take on a life of its own, where individuals may come to believe it based on their personal beliefs rather than whether or not it is true. Sometimes the best course of action is to do nothing.
- A sustained role for the public to engage in the development of this proposal, including through social media itself. The timing and approach to the public feedback process has discouraged input and analysis from a broad range of stakeholders with diverse and valuable perspectives. The government has not released any data to accompany these proposals. An approach such as that of the United Kingdom which published a White Paper two years before a draft bill with an extended time period for comment is encouraged.

2



- In order to be effective, this proposal needs to address the offline, real world components of radicalization, extremism and political campaigns.
- Consideration of cost. It is our sincere hope you release the revenue and costing estimates of this proposal publicly so they can be reviewed by experts in the field.

This submission will address key issues outlined in the discussion guide and technical paper released by Canadian Heritage.

Please don't hesitate to contact me if you have any questions about these recommendations.

Sincerely,

Michele Austin Manager | Public Policy (US & Canada) Twitter Inc.

\* details follow on next page

<sup>1</sup> Criminal Code (R.S.C., 1985, c. C-46), section 162.1

<sup>2</sup> Code section 163.1

- <sup>3</sup> Code sections 318 and 319
- <sup>4</sup> Code sections 83.21 and 83.22
- <sup>5</sup> Code section 319(1)

<sup>6</sup> An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service (S.C. 2011, c. 4)

https://mediaecosystemobservatory.com/press-release-canadian-election-misinformation-project-launch

#### ISSUE: PROACTIVE MONITORING AND "FLAGGING HARMFUL" CONTENT

Twitter's view is the framework proposed (beginning in module 1B of the technical paper) for proactive monitoring of content sacrifices freedom of expression to the creation of a government run system of surveillance of anyone who uses Twitter.

Even the most basic procedural fairness requirements you might expect from a government-run system such as notice or warning are absent from this proposal. The requirement to "share" information at the request of the Crown is also deeply troubling.

Twitter is committed to respecting the human rights of our users, in line with the expectations articulated in the <u>UN Guiding Principles on Business</u> and <u>Human Rights</u>. We have looked to internationally recognized human rights standards to guide our approach to content policy and enforcement, including those related to the protection of freedom of expression, privacy, security, non-discrimination, and to ensuring due process.

These rights are also enshrined in the Canadian Charter of Rights and Freedoms.

We value these approaches and standards in guiding how we navigate instances where rights may be in tension with one another. Each of our Twitter rules is designed to address specific harms on the platform. We try to ensure that content moderation actions we take are both necessary and proportionate to addressing such harms. We welcome further public discussion on how to ensure that regulatory frameworks are designed to prevent harm and reinforce broad equality rights as well as other fundamental human rights.

We support the spirit of the <u>Santa Clara Principles on Transparency and</u> <u>Accountability in Content Moderation</u> in considering how best to obtain meaningful transparency and accountability around government demands for increasingly aggressive moderation of user-generated content on Twitter.

At Twitter, we have identified our own responsibilities and limits. By using Twitter's services, you agree to be bound by our Terms of Service. Further, a user may not use our service for any unlawful purpose or in furtherance of illegal activities

In our continuing effort to make our services available to people everywhere, if we receive a valid and properly scoped request from an authorized entity, it may be necessary to withhold access to certain content in a particular country from time to time. Such withholdings are

4

limited to the specific jurisdiction that has issued the valid legal demand or where the content has been found to violate local law(s).

At Twitter, transparency is embodied in our open APIs, our information operations archive, and our disclosures in the Twitter Transparency Center. Tens of thousands of researchers access Twitter data we have made available over the past decade via our APIs. Most recently, we have offered a dedicated Covid-19 endpoint to empower public health research, and a new academic platform to encourage cutting edge research using Twitter data. Our archive of state-linked information operations is a unique resource and offers experts, researchers and the public insight into these activities.

In the long term, we believe a greater openness across the industry would be invaluable in delivering the transparency and accountability we all want to see.

Transparency is also vital to protecting freedom of expression. We have a notice policy for withheld content. Upon receipt of requests to withhold content, we promptly notify affected users unless we are prohibited from doing so (e.g., if we receive a court order under seal). When content has been withheld, we also clearly indicate within the product and publish requests to withhold content on Lumen—unless, similar to our practice of notifying users, we are prohibited from doing so.

"Flagging" will be used as a political tactic. As lived during the recent Canadian federal election, a general approach to flagging will result in censorship. Throughout the election campaign, political parties and their officials tried to have content "flagged" as "harmful" in an effort to have it removed from public discourse or score political points. Three of the many examples can be found <u>here</u>, <u>here</u> and <u>here</u>.

Further, individuals who report content should always be offered the option to remain safely anonymous. In some cases, there is a danger the reporter or the victim would be caught up and exposed via any national security investigation or in the sharing of information between governments or law enforcement agencies.

Our position on freedom of expression carries with it a mandate to protect our users' right to speak freely. While we may need to release information as required by law, we try to notify Twitter users before handing over their information whenever we can so they have a fair chance to fight the request if they so choose.

#### **ISSUE: 24 HOUR TAKEDOWN REQUIREMENTS**

Twitter opposes the recommendation of a time limit on "addressing" any content "flagged" by any person in Canada as "harmful" content.

- The proposed time limit does not allow for judicious, thoughtful analysis in a manner that balances the right to freedom of expression in Canada with the right to freedom from discrimination and prejudice.
- According to existing research and analysis, the proposed system has a high probability of negatively impacting marginalized, racialized and intersectional groups. More information from Prof. Suzie Dunn at Dalhousie University can be found <u>here</u>.
- The 24 hour proposal should be abandoned. Content should be addressed as quickly and as possible and within the scope of existing Canadian jurisprudence, terms of service and rules by the online communication service providers.
- Further, any standard applied in the digital world should also be applied in real life. For example, law enforcement should be required to both launch an investigation within 24 hours of "flagging" as well as remove any hateful content - graffiti on a statue for example - that appears within 24 hours across the country.

#### ISSUE: WEBSITE BLOCKING

The proposal by the government of Canada to allow the Digital Safety Commissioner to block websites is drastic. People around the world have been blocked from accessing Twitter and other services in a similar manner as the one proposed by Canada by multiple authoritarian governments (China, North Korea, and Iran for example) under the false guise of 'online safety,' impeding peoples' rights to access information online.

Further, there are no checks or balances on the commissioner's authority, such as the requirement of judicial authorization or warnings to service providers. The government should be extremely mindful of setting such a precedent - if Canada wants to be seen as a champion of human rights, a leader in innovation and in net neutrality globally, it must also set the highest standards of clarity, transparency and due process in its own legislation.

Clear guardrails must be put in place, and full assessments of potential unintended consequences should be undertaken before regulatory action is pursued. When this analysis takes place it must be released publicly.

#### ISSUE: WORKING WITH AND REPORTING TO LAW ENFORCEMENT AND OTHER AGENCIES

Twitter has an excellent working relationship with both the Royal Canadian Mounted Policy (RCMP) and the Canadian Security Intelligence Service (CSIS), which we value greatly.

We also work in partnership with the Canadian government though the Global Internet Forum to Counter Terrorism (GIFCT), the Christchurch Call to Action (CCTA), and the National Center for Missing and Exploited Children (NCMEC).

For example, Twitter already complies with domestic investigations of terrorist content and content that incites violence. Via Canada and Twitter's membership in GIFCT, we jointly announced in July that GIFCT is expanding its taxonomy database to capture terrorist manifestos. In the CCTA's *Crisis Response Work Plan*, Canada and Twitter both agreed to provide investigatory and prosecutory cooperation and trusted information exchanges, given that both are conducted in a manner that is consistent with the rule of law, has strong protections for human rights, and has relevant data protections and privacy regulations in tact.

The Government of Canada should not be using this proposal to grant CSIS or the Crown additional powers outside of those that are clearly identified in the CS/S Act. In addition, digital service providers are not an extension of Canadian law enforcement organizations.

If Twitter is required to preserve child sexual exploitation data beyond the NCMEC standard, Twitter will need clarity around what is required from the Government of Canada over and above what we currently provide. The feedback we have received from the RCMP is that our reporting is excellent. Industry practices vary widely and some peer companies do not submit the same set of data to NCMEC/the RCMP as Twitter.

Twitter will also need to consult and build out a new retention policy. We do not recommend holding this data indefinitely. Requirements for companies to hold on to personal data longer than necessary goes against best privacy practices and creates more risk of harm in the event of a breach.



### PUBLIC INTEREST ADVOCACY CENTRE LE CENTRE POUR LA DÉFENSE DE L'INTÉRÊT PUBLIC

285 McLeod Street, Suite 200, Ottawa, ON K2P 1A1

24 September 2021

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St, Gatineau QC K1A 0S5

BY EMAIL to: pch.icn-dci.pch@canada.ca

Re: The Government's proposed approach to address harmful content online- Submission of the Public Interest Advocacy Centre

Dear Consultation Secretariat Staff,

The Public Interest Advocacy Centre (PIAC) is pleased to provide the Government of Canada with our submission on the Government's proposed approach to address harmful content online, which is attached.

Sincerely,

John Digitally signed by John Lawford Lawford Date: 2021.09.24 19:43:39 -04'00'

John Lawford Executive Director & General Counsel 613-562-4002 jlawford@piac.ca Government's proposed approach to address harmful content online - Submission of the Public Interest Advocacy Centre 24 September 2021

### Introduction

The Public Interest Advocacy Centre (PIAC) is providing the below comments on the Government of Canada's proposed approach to regulating social media and combatting harmful content online ("Proposal"). PIAC is a national non-for-profit organization and registered charity that provides legal and research services on behalf of consumer interests, and, in particular, vulnerable consumer interests, concerning the provision of important public services. We are commenting narrowly on the possible impact that the Proposal's site-blocking feature may have on telecommunications consumers, but reserve the right to comment on any aspect of the Proposal at a later stage.

The Proposal states that the new legislation would apply to "online communication service providers" (OCSPs) and would include specific exemptions for telecommunications service providers (TSPs). PIAC supports this distinction and recommends that the government continue to draw an explicit line between OCSPs and TSPs. TSPs should not be able to circumvent their telecommunications duties under the *Telecommunications Act* by arguing that they are governed by the new regime under this Proposal.<sup>1</sup> The government should ensure TSPs continue to fulfill their obligations to telecommunications users as required by the laws and regulations overseen by the Canadian Radio-television and Telecommunications Commission (CRTC).

The Proposal suggests establishing a Digital Safety Commissioner and giving it the authority to apply, once all enforcement measures have been exhausted, to the Federal Court for an order requiring relevant TSPs to block access – in whole or in part – to an OCSP repeatedly demonstrating persistent non-compliance with orders respecting the removal of child sexual exploitation content or terrorist content. The Proposal states that s.36 of the *Telecommunications Act* will not apply to Canadian carriers that comply with these blocking orders and does not plan to repeal or amend this section.

With the exception of child sexual exploitation content, which is already *de facto* censored by the Cybertip.ca Cleanfeed project, PIAC does not believe that site-blocking is an appropriate mechanism to address the online harms identified in the Proposal. If the Proposal is to create an avenue for site-blocking we suggest that the CRTC be the decision-maker, so as to ensure that site-blocking does not undermine Canada's telecommunications system nor impair Canadian's rights to telecommunications services. If the government decides to make the Federal Court the site-blocking adjudicator we suggest that it create explicit requirements that the court consider s. 36 and s. 27(2) rulings and jurisprudence and issue orders that apply narrowly to the conduct of

<sup>&</sup>lt;sup>1</sup> As an example of attempted circumvention, in Broadcasting and Telecom Decision CRTC 2015-26, Bell Mobility and Videotron attempted avoid application of the *Telecommunications Act* by arguing they were broadcasting undertakings when offering mobile TV services rather than TSPs, despite the fact that subscribers needed to have a mobile wireless voice plan, data plan, or tablet plan in order to access mobile TV services. The CRTC rightfully concluded that the two companies were providing telecommunications services and thus subject to the *Telecommunications Act*.

Government's proposed approach to address harmful content online - Submission of the Public Interest Advocacy Centre 24 September 2021 cific parties before them in order to safeguard Canada's telecommunications system and

the specific parties before them in order to safeguard Canada's telecommunications system and the CRTC's role in regulating it.

# ISP site-blocking is not an appropriate mechanism to address online harms

PIAC submits that it is likely not appropriate to create a regime in which ISPs are required by court order to block user access to non-compliant OCSPs because mandatory site-blocking: 1) is incompatible with Canada's net neutrality framework rooted in ss. 36 and 27(2) of the *Telecommunications Act* as articulated by the CRTC; and 2) could result in excessive infringement of Canadians' rights to freedom of expression on the Internet.

## Incompatibility with Canada's net neutrality framework

Net neutrality is the concept that all data traffic on a network should be treated indiscriminately and that internet service providers (ISPs) should be restricted from blocking, slowing down or speeding up the delivery of online content at their discretion. There are many iterations of net neutrality around the world and determining the scope of net neutrality requires looking specifically at the ways ISPs are regulated within the relevant jurisdiction. In Canada, the CRTC has stated that the following documents make up Canada's net neutrality framework: Telecom Regulatory Policy CRTC 2017-104 (*Differential pricing practices*), Telecom Decision CRTC 2017-105 (*Videotron unlimited music*), Broadcasting and Telecom Decision CRTC 2015-26 (*Bell Mobile TV*), and Telecom Regulatory Policy CRTC 2009-657 (*Internet traffic management practices*).<sup>2</sup> Underlying this framework are the factors upon which public support for net neutrality is built: competition, innovation, consumer choice, access and affordability, and privacy.<sup>3</sup>

Canada's net neutrality framework is rooted in ss. 27(2) and 36 of the *Telecommunications Act*, which must be interpreted and applied to further the telecommunications policy objectives set out in section 7 of the *Telecommunications Act*.

Section 27(2) prohibits Canadian carriers from unjustly discriminating or giving undue or unreasonable preference or disadvantage to any person, including itself and competitors. The CRTC has set out four criteria for considering whether preference is undue or unreasonable in the context of differential price setting:

- the degree to which the treatment of data is agnostic (i.e. data is treated equally regardless of its source or nature);
- whether the offering is exclusive to certain customers or certain content providers;

 <sup>&</sup>lt;sup>2</sup> Telecom Regulatory Policy CRTC 2017-104, Framework for assessing the differential pricing practices of Internet service providers, 20 April 2017 [Differential pricing practices].
 <sup>3</sup> Ibid, at para 32.

Government's proposed approach to address harmful content online - Submission of the Public Interest Advocacy Centre 24 September 2021

- · the impact on Internet openness and innovation; and
- whether there is financial compensation involved.<sup>4</sup>

Using these criteria, the CRTC has previously held that zero-rating data charges associated with a category of content resulted in undue preference/disadvantage.<sup>5</sup> Since the impact of outright blocking is greater than differential price setting it follows that blocking would also unduly disadvantage website users and operators, who are unable to obtain or provide the content they wish to obtain or provide. The user is unduly disadvantaged relative to a user accessing other content, and the operator is unduly disadvantaged relative to operators who run other sites. Implementing a site-blocking regime may also potentially disadvantage smaller or newer ISPs, who may be less able to absorb the cost of updating their networks to enable blocking. The extent of these costs will depend on what blocking system is ordered and how the list of non-compliant OCSPs is maintained and updated. The government should be mindful of placing additional burden on ISPs, particularly smaller or newer ones, in order to ensure the public has access to adequate levels of choice and competition is sufficient to drive innovation. Lastly, while there are not, to our knowledge, vertically integrated ISPs and OCSPs such a possibility may present itself in future, at which point there will likely be additional concerns regarding impacts on competition and also freedom of expression, as ISPs will have financial incentive to suppress content on non-affiliate OCSPs.

Section 36 of the *Telecommunications Act* limits the ability of Canadian carriers to control the content or influence the meaning or purpose of telecommunications carried over their networks without prior CRTC authorization, but does not give the CRTC the power to require TSPs to block content. In the 2018 *FairPlay Decision,* the CRTC stated: "section [36] gives the Commission the explicit power to authorize an ISP to block a website, the proposed regime would go further and require such blocking pursuant to a Commission order. Because section 36 confers an authorizing power and not a mandatory power, the power to mandate blocking must be found elsewhere..."

The CRTC then determined it is only able to approve ISP content blocking if doing so will further the telecommunications policy objectives in s. 7, under certain circumstances. In the context of Internet traffic management practices, the CRTC has stated:

122. The Commission finds that where an ITMP would lead to blocking the delivery of content to an end-user, it cannot be implemented without prior Commission approval. Approval under section 36 would only be granted if it would further the telecommunications policy objectives set out in section 7 of the Act. Interpreted in light of these policy objectives, ITMPs that result in blocking

<sup>4</sup> Ibid. at para. 126.

<sup>&</sup>lt;sup>5</sup> Telecom Decision CRTC 2017-105, Complaints against Quebecor Media Inc., Videotron Ltd., and Videotron G.P. alleging undue and unreasonable preference and disadvantage regarding the Unlimited Music program, 20 April 2017.

<sup>&</sup>lt;sup>6</sup> Telecom Decision CRTC 2018-384, Asian Television Network International Limited, on behalf of the FairPlay Coalition – Application to disable online access to piracy websites, 2 October 2018, at para. 69 [FairPlay Decision].

Government's proposed approach to address harmful content online - Submission of the Public Interest Advocacy Centre 24 September 2021

Internet traffic would only be approved in exceptional circumstances, as they involve denying access to telecommunications services.

Similarly, in Telecom Decision CRTC 2016-479 the CRTC affirmed, in the context of Quebec's attempt to block access to unauthorized gambling websites, that "blocking would only be approved where it would further the telecommunications policy objectives set out in section 7 of the Act."<sup>7</sup> The CRTC did not find that Quebec's actions would further these objectives but, rather, would impede them.

The Supreme Court of Canada has summarized the purpose of the *Telecommunications Act* in light of its policy objectives as being "to encourage and regulate the development of an orderly, reliable, affordable and efficient telecommunications infrastructure for Canada."<sup>8</sup> PIAC submits that blocking the delivery of almost any content to end-users is fundamentally at odds with the policy objectives set out in s. 7. A TSP that blocks content requested and transmitted over their network effectively is an unreliable service provider providing sub-standard service from a user point of view. The very point of an ISP, indeed, the reason a contract exists between the ISP and the user, and what the ISP accepts monetary compensation for, is to provide access to the Internet and to carry traffic over the ISPs' network to and from the wider Internet.

Section 7(i) of the *Telecommunications Act* requires telecommunications policy to "contribute to the protection of the privacy of persons". Further, the CRTC has stated that it

"recognizes that [Virtual Private Networks] VPNs are a legitimate tool to protect sensitive information, as recommended by security firms. While the Commission does not find differential pricing practices to have a direct negative impact on privacy per se, it is concerned that their adoption could discourage the use of VPNs and thus compromise the privacy and/or security of consumers.<sup>9</sup>

The CRTC has consistently held that subs. 7(i) permits the Commission to create higher privacy obligations in relation to confidential customer information in telecommunications than is required in general Canadian privacy law.<sup>10</sup>

Upholding individuals' ability to protect their privacy through VPNs and other encryption methods may make site-blocking an ineffective tool for preventing access to non-compliant OCSPs and these tools may, under the CRTC's approach to privacy under subs. 7(i), be held to be an important aspect of telecommunications' users' privacy. There are a variety of ways users, even technically unsophisticated ones, may easily circumvent blocked access to websites. One method of blocking websites is to program the Domain Name System (DNS) server to refuse to translate the URL into an IP address. When a person looks up a website, they enter a URL

<sup>&</sup>lt;sup>7</sup> Telecom Decision CRTC 2016-479, Public Interest Advocacy Centre – Application for relief regarding section 12 of the Quebec Budget Act, at para. 7 [Telecom Decision, Quebec Budget Act].

<sup>&</sup>lt;sup>8</sup> FairPlay Decision, supra note 4 at para. 69, citing Barrie Public Utilities v. Canadian Cable Television Assn., [2003] 1 SCR 476, at paragraph 38.

<sup>&</sup>lt;sup>9</sup> Differential pricing practices, supra note 5 at para. 78.

<sup>&</sup>lt;sup>10</sup> See: Telecom Decision 2003-33 and 2003-33-1, Confidentiality provisions of Canadian carriers. Online: <u>https://crtc.gc.ca/eng/archive/2003/dt2003-33.htm</u>

#### Environmental Martin Sciences International Constraints Sciences Sciences and Sciences and International International According Sciences (2019) 1010–1012 (2019) International Sciences (2019) 1010–1012 (2019) International Sciences (2019)

#### Government's proposed approach to address harmful content online - Submission of the Public Interest Advocacy Centre 24 September 2021

including a domain name (ex. Google.ca). A DNS server translates domain names into an IP address which can be used to communicate directly with the websites. Most ISPs have their own DNS servers, which customers may, and most do use (although a technically sophisticated user can specify their preferred DNS server to be one other than that of their ISP). DNS-based blocking can be easily circumvented by entering the IP address directly, using a proxy, using another DNS server or following a link to the IP address. Another method is to block the IP address. This can be easily circumvented by users by using a VPN, which hides the destination of web traffic from the internet service provider. IP blocking is also easy for the site operator to circumvent by changing their IP addresses. A third method is to inspect the packets of data to determine their destination and block packets destined for the infringing website Deep-packet inspection can be easily circumvented by encrypting web-traffic. End users do not have to understand these circumvention measures to use them. Through software users can establish encrypted private network connection with a non-compliant OCSP which an internet service provider cannot block.

The Proposal's indication that ISPs may be required to block access to only a part of a noncompliant OCSP leads PIAC to presume that deep-packet inspection would be a necessary blocking method. Deep-packet inspection would require ISPs to examine aspects of packets which they would not otherwise examine and use that information to make a decision about whether the packet should be permitted to pass. These additional steps may impose undue burden on ISPs potentially impacting network performance and competition among telecommunications companies. Deep-packet inspections may also constitute an unreasonable search if they reveal private information about users, for example, their financial, medical, or personal information, which is at the heart of the "biographical core" protected by s.8 of the *Charter.*<sup>11</sup>

Finally, the CRTC has forbidden, on the basis of users' confidentiality interests, ISPs' use of deep packet inspection for any purpose except traffic management:

103. In light of the above, the Commission finds it appropriate to establish privacy provisions in order to protect personal information. The Commission therefore directs all primary ISPs, as a condition of providing retail Internet services, not to use for other purposes personal information collected for the purposes of traffic management and not to disclose such information.<sup>12</sup>

<sup>&</sup>lt;sup>11</sup> Depending on the context, Canadians have a reasonable expectation of privacy in their identity as the internet subscriber associated with particular usage (R v Spencer 2014 SCC 43) and in their personal digital devices (R v Fearon 2014 SCC 77) and in electronic conversations (R. v. Marakah 2017 SCC 59; R. v. TELUS Communications Co. 2013 SCC 16), and personal computers (R. v. Morelli 2010 SCC 8) and work computers where personal use is permitted (R. v. Cole 2012 SCC 53).

<sup>&</sup>lt;sup>12</sup> Telecom Regulatory Policy CRTC 2009-657, *Review of the Internet traffic management practices of Internet service providers* (21 October 2009), at para. 103.

Government's proposed approach to address harmful content online - Submission of the Public Interest Advocacy Centre 24 September 2021

It is not surprising, therefore, that given the scope of ss. 27(2) and 36 that the CRTC has yet to approve a site-blocking request, even in situations of alleged harm.<sup>13</sup> PIAC submits that nothing in the *Telecommunications Act* nor the net neutrality framework articulated by the CRTC provides an exception to allow site-blocking merely because content is criminal or, to use the language of the Proposal, harmful. As this section of our comments highlights, ss. 27(2) and 36 have been interpreted in such a way as to require ISPs to treated content agnostically and not prefer, restrict, slow, or block content unless the CRTC authorize them to do so, having determined that differential treatment or restricted access will further the objectives of telecommunication policy. Any argument that restricting access to a subset of non-compliant OCSPs has only an incidental interference with the provision of telecommunications service is untenable. The nature of Internet activity is that it is personal to the user. The government, CRTC, ISP, and OCSP do not know the extent to which users, those engaging in harmful content and those not, rely on the OCSP that is to be restricted. Restricting access could have the effect of seriously impeding service if a customer only or predominantly uses the Internet to access the blocked websites.

## Potential Impact on Freedom of Expression

The CRTC has acknowledged the role of Internet access in safeguarding, enriching, and strengthening Canada's "social and economic fabric."<sup>14</sup> Free expression on the Internet is fundamental to this fabric and, according to a Joint Declaration by the UN Special Rapporteur for Freedom of Opinion and Expression and the IACHR-OAS Special Rapporteur on Freedom of Expression:

[A]II restrictions on freedom of expression, including those that affect speech on the Internet, should be clearly and precisely established by law, proportionate to the legitimate aims pursued, and based on a judicial determination in adversarial proceedings. In this regard, legislation regulating the Internet should not contain vague and sweeping definitions or disproportionately affect legitimate websites and services.

PIAC submits that government mandated website blocking necessarily engages s. 2(b) of the *Canadian Charter of Rights and Freedoms* and this right ought to be considered by the government in the context of the Proposal. We find support for this position in s. 41(1) of the *Telecommunications Act*, which requires the CRTC consider freedom of expression when

<sup>&</sup>lt;sup>13</sup> As an example, in a Letter Decision from Diane Rheaume, Secretary General of the CRTC to J. Edward Antecol dated 24 August 2006 (file no. 8622-P49-200610510), the CRTC declined an application purportedly made under s. 36 to have the Commission proactively authorize ISPs to block certain websites alleged to constitute hate speech. The applicant provided expert evidence in support of his view that the two websites in question violated the *Criminal Code*. He also claimed that the websites, having posted his home address and made repeat and violent anti-Semitic statements, cause him to fear for his personal safety and the community at large. The CRTC reiterated that s.36 could not be used to require ISPs to block access to websites and denied the Application for procedural reasons.

<sup>&</sup>lt;sup>14</sup> For example, Telecom Regulatory Policy CRTC 2016-496, *Modern telecommunications services – The path forward for Canada's digital economy*, 21 December 2016 at para. 21.

#### Government's proposed approach to address harmful content online - Submission of the Public Interest Advocacy Centre 24 September 2021

deciding to prohibit or regulate unsolicited telecommunications to prevent undue inconvenience or nuisance.

Canadians have a right to "freedom of [...] expression, including freedom of the press and other media of communication." The fundamental values underlying the guarantee of freedom of expression were well articulated by McLachlan J's dissent (not on this point) in *R v Keegstra* [1990] 3 SCR 697. To paraphrase, the main justifications for freedom of expression are:

- The free flow of ideas is essential to political democracy and the functioning of democratic institutions.
- 2. A marketplace of ideas leads to a more relevant, vibrant, and progressive society.
- 3. People have a fundamental right to their own beliefs and opinions, and to express them, and such expression contributes to the self-realization of both speaker and listener.

What constitutes protected expression under Supreme Court of Canada jurisprudence is quite broad and includes non-violent hate speech<sup>15</sup> and child pornography.<sup>16</sup> Both types of expression have been limited via *Criminal Code* prohibitions in ways that have been held demonstrably justifiable in a free and democratic society and PIAC is not arguing that it is impossible for the government to further restrict these forms of expression in justifiable ways. However, we want to raise our concerns about the potential issues with the Proposal's site-blocking regime in relation to freedom of expression.

Harm is often dependent on one's perception. PIAC took the position that net neutrality does not warrant special treatment for harmful or even criminal content in relation to disabling access to sites hosting content allegedly infringing copyright<sup>17</sup> and in relation to Bill 74 which purported to allow the Province of Québec to require ISPs to block access to 'unauthorized' gambling websites within 30 days of receipt of notice from Quebec.<sup>18</sup> In the former instance, copyright holders argued access to content allegedly infringing copyright was harmful, but some users, site operators, and ISPs disagreed. In the latter, the government of Quebec claimed unauthorized online gambling websites were harmful because they did not contain the same responsible gaming rules as sites run by the government. However, the province also embedded the site-blocking regime in a budgetary bill and made it clear that blocking access to unauthorized websites would generate significant revenue, thus demonstrating how the concept of harm can be used to mask other aims. Reasonable people can disagree about the value of various forms of expression and whether such expression ought to be suppressed to prevent harm.

For example, the Proposal suggests that users may be blocked from accessing OCSPs that are repeatedly non-compliant in blocking access to "terrorist content" and that the definition of this harm will be based on the *Criminal Code*. The *Criminal Code* contains a definition of "terrorist

<sup>15</sup> R v Keegstra [1990] 3 SCR 697.

<sup>&</sup>lt;sup>16</sup> R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R. 45; R. v. Barabash, 2015 SCC 29, [2015] 2 S.C.R. 522.

<sup>&</sup>lt;sup>17</sup> FairPlay Decision, supra note 4 at para. 67

<sup>&</sup>lt;sup>18</sup> Telecom Decision, Quebec Budget Act, supra note 10.

#### Free and the Constant of the Second Second In the Annual Constant of Distribution of the Second Second Second Second Second Diff. Here 2: A constant of Second Second Diff. 30 (2017) 10 (2017) 10 (2017)

#### Government's proposed approach to address harmful content online - Submission of the Public Interest Advocacy Centre 24 September 2021

activity" which, to paraphrase, requires: 1) an act or omission; 2) committed, at least in part, for a political, religious, or ideological purpose; 3) with some intention to intimidate the public with regard to its security, including economic security, or with some intention to compel a person, government, or organization to do or refrain from doing any act; and 4) that intentionally a) causes death or serious bodily harm through violence, b) endangers a person's life, c) causes a serious risk to the health or safety of the public, d) causes substantial property damage, whether to public or private property, or e) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to cause death or bodily harm or endanger a person's life. PIAC is concerned that there may be instances where it is difficult to distinguish between legitimate forms of expression and terrorist content. For example, protest and work stoppages are excluded from the above definition, but it is not clear if they would be captured under "terrorist content" if, for example, the content depicted people seriously disrupting an essential service with the intention of compelling a government or organization to respond to protest or labour demands, both of which are made for an ideological purpose. PIAC recommends that the government provide more information, after consultation with civil liberties societies and minorities' rights groups, on how it intends to ensure that the scope of content to be blocked under the category of "terrorist content" does not capture otherwise legitimate forms of expression, including advocacy, protest, dissent, and work stoppages, which may, depending on one's political perspective, resemble terrorist activity. PIAC also recommends that the government consider safeguards to ensure that governments, corporate interests, and majority groups are not able to use the proposed site-blocking regime to suppress expression that threatens their power by, for example, repeatedly complaining about OCSP non-compliance and having these complaints entertained by the Digital Safety Commissioner, whose level of independence is not clear from the Proposal. As former CRTC National Commissioner Timothy Denton, as he then was, wrote: "History shows that schemes of regulation - and censorship have a tendency to expand [...]."<sup>19</sup> PIAC is concerned that over time more and more content may be restricted, under the guise of harm, to suit the desires of the state.

Content that sexually exploits children is nearly universally accepted as harmful and PIAC is not against blocking access to child pornography. However, PIAC wonders why they government has not acknowledged that Canada's major ISPs already voluntarily block customer access to non-Canadian websites that are hosting child pornography using Cleanfeed Canada, an undertaking of the Canadian Coalition Against Internet Child Exploitation (CCAICE).<sup>20</sup> ISPs currently perform this blocking without, to our knowledge, legislated authority.<sup>21</sup> PIAC suggests the government consider regulating this existing practice and determining what needs to be

 <sup>&</sup>lt;sup>19</sup> Broadcasting Regulatory Policy CRTC 2009-329, *Review of broadcasting in new media*, 4 June 2009, Concurring opinion of Commissioner Timothy Denton (Revised as of 8 July 2009).
 <sup>20</sup> Cybertip.ca, "Cleanfeed Canada" online: <a href="https://www.cybertip.ca/app/en/projects-cleanfeed">https://www.cybertip.ca/app/en/projects-cleanfeed</a>>.

<sup>&</sup>lt;sup>21</sup> Cybertip.ca, Clearneed Canada Online. <a href="https://www.cybertip.ca/app/en/projects-clearneed">https://www.cybertip.ca/app/en/projects-clearneed</a>.
<sup>21</sup> Cybertip.ca states: "ISPs do not consider themselves qualified to determine the legality of content. The Criminal Code allows a judge to make such legal determinations for child pornography content on the Internet, and to issue take-down orders if such content is hosted in Canada. ISPs follow this legislation and rely on the courts for direction. There is no such legislation for child pornography content hosted outside of Canada, so filtering access based on the Cybertip.ca list is an effective way to deal with such foreign content."

Government's proposed approach to address harmful content online - Submission of the Public Interest Advocacy Centre

24 September 2021

done in order to use this system to further reduce Canadian's exposure to child abuse images and create a disincentive for those who access and distribute child pornography in a way that is effective, proportional, and results in minimal impairment to expression that does not constitute child exploitation.

Since justifying infringement of a *Charter* right requires an assessment of whether the measures selected are rationally connected to the aim of the legislation, which in this instance is reducing public exposure to terrorist content and child exploitation content, PIAC's comments regarding the potential ineffectiveness of site-blocking mentioned in the previous section are also relevant to the discussion of freedom of expression.

Recommendations if the government is to move forward with a

mandatory site-blocking regime

PIAC does not believe it is appropriate to create a site-blocking regime that will require ISPs to block access to non-compliant OCSPs. However, if the government is to create an avenue for site-blocking, PIAC suggests that the CRTC be the decision-maker so as to ensure that Canadians' right to telecommunications services and right to freedom of expression, as discussed above, are not unduly restricted.

In its 2018 *FairPlay* Decision, the CRTC stated that s. 36 "gives the Commission the explicit power to authorize an ISP to block a website, [but that] the proposed regime would go further and require such blocking pursuant to a Commission order. Because section 36 confers an authorizing power and not a mandatory power, the power to mandate blocking must be found elsewhere..."<sup>22</sup> The government would, therefore, need to amend the *Telecommunications Act* to provide the CRTC with the ability to issue site-blocking orders on application from not only Canadian carriers, but other interested parties, including, presumably, the Digital Safety Commissioner. This amendment would provide the CRTC with the authority to consider and, in very limited instances, issue mandatory site-blocking orders in ways that are congruent with telecommunications law and policy.

PIAC cautions that creating a court ordered site-blocking regime may produce results inconsistent with the CRTC's existing, approval-based site-blocking regime if, for example, an ISP seeking to block content via CRTC approval is denied, but the Digital Safety Commissioner is subsequently granted a Federal Court site-blocking order requiring the ISP to block content. Since the CRTC's decisions are based on telecommunications policy considerations such an inconsistence may undermine Canada's telecommunications system. That said, if the government intends to make a court ordered site-blocking regime, we suggest that it include explicit requirements that the court consider s. 36 and s. 27(2) rulings and jurisprudence and

<sup>&</sup>lt;sup>22</sup> Telecom Decision CRTC 2018-384, Asian Television Network International Limited, on behalf of the FairPlay Coalition – Application to disable online access to piracy websites, 2 October 2018, at para. 69 [FairPlay Decision].

Government's proposed approach to address harmful content online - Submission of the Public Interest Advocacy Centre 24 September 2021

issue orders that apply narrowly to the conduct of the specific parties before them in order to safeguard Canada's telecommunications system and the CRTC's role in regulating it.

PIAC notes that the Federal Court of Appeal (FCA) recently affirmed the availability of mandatory interlocutory injunctions as a means of blocking online access to content allegedly infringing copyrighted materials in Canada.<sup>23</sup> In the absence of parliamentary intervention, siteblocking orders will likely be issued based on the factors identified by Mr. Justice Gleeson in *Bell Media Inc. v. GoldTV.Biz*, 2019 FC 1432 not only in the context of online 'piracy', but online harms as well.

PIAC is not commenting on the general appropriateness of these factors,<sup>24</sup> but submits that they may be insufficient to safeguard Canada's net neutrality framework and Canadains' right to freedom of expression, noted above, especially given Mr. Justice Gleeson's consideration of these issues – upheld by the FCA – was as follows:

"I am not prepared to conclude, as the Plaintiffs have suggested, that the principle of net neutrality is of no application where a site-blocking order is sought. However, I am satisfied, in the face of a strong *prima facie* case of ongoing infringement and a draft order that seeks to limit blocking to unlawful sites and incorporates processes to address inadvertent over-blocking that neither net neutrality nor freedom of expression concerns tip the balance against granting the relief sought. As has been previously noted by the Supreme Court of Canada, albeit in a different context, the jurisprudence has not, to date, accepted that freedom of expression requires the facilitation of unlawful conduct (*Equustek* at para 48). Similarly I am not convinced that the principle of net neutrality, or the common carrier doctrine, is to be applied in a manner that requires ISPs to facilitate unlawful conduct."<sup>25</sup>

PIAC also notes that court ordered site-blocking can be impractical and burdensome. Mr. Justice Gleeson's site-blocking order has been updated several times to expand the list of domains to be blocked and remove domains no longer being used to provide access to the allegedly copyright-infringing content.<sup>26</sup> PIAC is not surprised by this outcome because, as we have described above, site operators and users can easily circumvent domain and IP address blocking. Also noted above is our understanding that smaller ISPs may be disproportionately impacted by the costs associated with ongoing and rapidly change blocking requirements. The

25 Bell Media Inc. v. GoldTV.Biz, 2019 FC 1432 at para. 97.

<sup>26</sup> The Wire Report, "Site-blocking in GoldTV case expanded again" (Sept 2021), online: <a href="https://www.thewirereport.ca/2021/09/15/site-blocking-in-goldtv-case-expanded-again/">https://www.thewirereport.ca/2021/09/15/site-blocking-in-goldtv-case-expanded-again/>. Scorrowski and Allocards In-

<sup>23</sup> Teksavvy Solutions Inc. v. Bell Media Inc., 2021 FCA 100.

<sup>&</sup>lt;sup>24</sup> Mr. Justice Gleeson used factors cited in United Kingdom jurisprudence and codified by the United Kingdom parliament in *Copyright, Designs and Patents Act 1988.* At the irreparable harm stage, Gleeson J. considered whether the injunction was necessary to protect the plaintiff's rights and the availability of alternative and less onerous measures. In weighing the balance of convenience he considered: effectiveness; dissuasiveness; complexity and cost' barriers to legitimate use or trade; fairness, including a brief note on freedom of expression and net neutrality; substitution; and safeguards.

Government's proposed approach to address harmful content online - Submission of the Public Interest Advocacy Centre 24 September 2021

issues of practicality and burden have broader implications on telecommunications law and policy and, therefore, would be more properly addressed by the CRTC.

PIAC notes that Bell, Rogers, and Quebecor are requesting the Federal Court establish Canada's first-ever "dynamic" site-blocking order, which would require third-party ISPs to block a rolling list of IP addresses in real-time, as they are identified by the broadcasters as broadcasting 'pirated' National Hockey League games while those games are being broadcast throughout the NHL season.<sup>27</sup> If granted this order would require proactive content blocking, which is problematic for reasons discussed in our comment. This request demonstrates the growing need for the government, if it is to have court ordered site-blocking, to set parameters to minimize the impact of such decision on Canada's telecommunications system.

PIAC notes that Teksavvy is appealing the FCA decision to the Supreme Court of Canada arguing, in part, that judicial site-blocking "risks displacing and overtaking Parliament's carefullycrafted statutory regime..." and is "incompatible with the statutorily mandated neutrality of ISPs as common carriers..."<sup>28</sup> PIAC awaits the result of this appeal as should the government, before moving forward with legislation requiring ISPs to block content.

#### Conclusion

PIAC reiterates that site-blocking we believe it is inappropriate to use site-blocking to address the online harms identified in the Proposal, except in so far as to legislate and expand upon the existing practice of ISP's blocking access to non-Canadian websites that are hosting child pornography using Cleanfeed Canada.

If the Proposal is to create an avenue for site-blocking we suggest that the CRTC be the decision-maker so as to ensure that site-blocking does not undermine Canada's telecommunications system nor impair Canadian's rights to freedom of expression.

If the government makes the Federal Court the site-blocking adjudicator we suggest that it provide explicit requirements that the court consider s. 36 and s. 27(2) rulings and jurisprudence and issue narrow orders that apply only to the conduct of the specific parties before them in order to safeguard the role of the CRTC and Canada's telecommunications system. As stated in the introduction, PIAC may voice our additional concerns about the Proposal at a later stage, particularly our concerns about: mandatory OCSP reporting to law enforcement and CSIS; extended data retention periods; expansion of the *Mandatory Reporting Act* to require

<sup>&</sup>lt;sup>27</sup> The Wire Report, "Bell, Rogers, and Quebecor seek first-ever 'dynamic' site-blocking order"(July 2021), online: <a href="https://www.thewirereport.ca/2021/07/08/bell-rogers-and-quebecor-seek-first-ever-dynamic-site-blocking-order/">https://www.thewirereport.ca/2021/07/08/bell-rogers-and-quebecor-seek-first-ever-dynamic-site-blocking-order/</a>.

<sup>&</sup>lt;sup>28</sup> Chris Cooke, "Canadian ISP takes web-blocking debate to the country's Supreme Court" (Aug 2021), online: <a href="https://completemusicupdate.com/article/canadian-isp-takes-web-blocking-debate-to-the-countrys-supreme-court/">https://completemusicupdate.com/article/canadian-isp-takes-web-blocking-debate-to-the-countrys-supreme-court/</a>.

Government's proposed approach to address harmful content online - Submission of the Public Interest Advocacy Centre 24 September 2021 provide basic subscriber information to law enforcement; and the proposed

ISPs to provide basic subscriber information to law enforcement; and the proposed administrative structure.

For now, we have limited our comments to the possible impact of the Proposal's site-blocking regime on telecommunications consumers. We ask that in considering whether and how to implement such a regime that the government consider the broader implications on Canada's net neutrality framework, including the effects on competition, innovation, consumer choice, access and affordability, privacy, and Canadians' right to freedom of expression.

\*\*\* End of Document \*\*\*

Gossenment commonique en virrai en la Esti avir conces à l'Universitaire Disconsent mésosiet dominant la Dis Access la minamministria et



## NATIONAL COUNCIL OF CANADIAN MUSLIMS

## CONSEIL NATIONAL DES MUSULMANS CANADIENS

Your Voice. Your Future.

Votre voix. Votre avenir.

BRIEF ON ONLINE HATE: Responding to the Proposed Approach to Address Harmful Content Online

#### DEPARTMENT OF CANADIAN HERITAGE

GOVERNMENT OF CANADA | SEPTEMBER 24, 2021

hanstanten er en sterkte poor op oorden. Asterne geveen geskerse belaande en op Maangengelen de anderer en gebeure de Die die eeste de anterer maarte oorde

#### I. Introduction

The National Council of Canadian Muslims (NCCM) is an independent, non-partisan and non-profit organization that protects Canadian human rights and civil liberties, challenges discrimination and Islamophobia, builds mutual understanding, and advocates for the public concerns of Canadian Muslims.

#### II. Summary

While we are supportive of the general framework set forward in the proposed legislation, we would have grave concerns (generally summarized) if a copy of all reports and associated information of online hate automatically get sent to law enforcement.

In other words, the components that make reference to "terrorist content" need to be removed from the draft online hate bill. These components are, to us, a rehashing of the problems of Bill C-51. If these provisions are not removed, we will likely have to be in the position of publicly opposing this bill. Frankly, we are disappointed that these provisions were even anticipated in the consultation package, since we have been very clear in our discussions that this would have obvious problems.

This is not something we want, as we are very supportive of the need for online hate regulation that is balanced and respects our civil liberties.

#### III. Why We Support Online Hate Reform

On the evening of July 29, 2017, six Canadian Muslims were murdered and 19 injured in the midst of their prayers at the Centre Culturel Islamique de Québec in Ste. Foy, Quebec by Alexandre Bissonnette.

Ibrahima Barry. Azzedine Soufiane. Aboubaker Thabti. Khaled Belkacemi. Mamadou Tanou Barry. Abdelkarim Hassane. In an instance of hate and violence, their earthly presence was removed from us in what remains the worst attack on a house of worship on Canadian soil.

In *R. c. Bissonnette*, 2019 QCCS 354, Justice François Huot indicated at paragraphs 10-12 of the decision that Bissonnette drew upon online sources before committing this horrific attack:

[10] ...il consulte assidûment divers sites Internet portant, notamment sur les armes à feu et auteurs d'actes terroristes. À titre d'exemples, il accède, le 27 janvier, au compte Twitter de #Muslimban...

[11] Le lendemain, il fait diverses lectures sur Jaylen Fryberg, l'auteur de la tuerie de Marysville, Elliot Rodger, responsable de la tuerie de masse du 23 mai 2014 à Isla Vista en Californie, Dylann Roof, l'assassin de neuf Afro-Américains lors de la fusillade de l'église de Charleston, l'attaque de San Bernardino et la page Facebook du mouvement FÉMUL (Féministes en mouvement de l'Université Laval).

[12] Dans la matinée du 29 janvier 2017, Bissonnette déjeune en consultant d'autres sites traitant d'attentats djihadistes...

#### [Translated to English]

[10] During this same period, he regularly consulted various Internet sites relating, in particular, to firearms and perpetrators of terrorist acts. For example, on Jan. 27, he accessed #Muslimban's Twitter account...

[11] The following day, he made various readings on Jaylen Fryberg, the author of the Marysville slaughter, Elliot Rodger, mass murderer of May 23, 2014 in Isla Vista, California, Dylann Roof, the murderer of nine African Americans during the shooting of the Charleston church, the San Bernardino attack and the Facebook page of the FÉMUL movement (Feminists in Motion at Laval University).

[12] On the morning of January 29, 2017, Bissonnette consulted other sites dealing with jihadist attacks...

There is no clearer indication to us that online hate poses as existential threat to Canadians, and to Canadian security. An analysis of his computer records showed that Bissonnette, from December 27, 2016 to January 29, 2017, consulted various sources about Islam on the internet. While we do not propose that Bissonnette was solely motivated by online hate speech or online racist manifestos, it is clear that Bissonnette consulted these online sources before committing his attack. That is simply part of the evidence.

In Canada, there is little doubt from an empirical perspective that online hate, primarily through social media, but also through blogs, podcasts, other websites, and the dark web continues to fuel animosity and Islamophobia towards Canadian Muslim populations. Online hate stokes animosity, fear, and promotes misinformation and anti-

Semitism against our friends and allies in the Jewish community as well. The scourge of white supremacy, as well as the "incel" community, has been given a revival and a rebirth by way of the growth of social media, where misinformation and hate pose an existential threat to Canadian security.

In 2016, media research company Cision documented a 600% rise in the amount of intolerant and hate speech in social media postings between November 2015 and November 2016. Their study focused on the usage of hashtags like #banmuslims and #siegheil.<sup>1</sup> According to a 2019 survey by Leger Marketing, 60% of Canadians report having seen hate speech on social media, and 62% of Quebecers stated that they had seen hateful or racist speech on the internet/social media in relation to Muslims.<sup>2</sup>

There is far more empirical data demonstrating this point than can be adequately condensed into this brief. Perry and Scriven's research on how Canadian hate groups (like Blood and Honour or the Canadian Nationalist Front) utilize online platforms, including social media platforms, demonstrates that white supremacist and online hate groups use online platforms to create an "enabling environment".<sup>3</sup> Groups like the Soldiers of Odin (founded by a neo-Nazi), Pegida Canada, and other organizations routinely use Twitter and Facebook as organizing tools, as well as to continue to spread misinformation and hate about immigrants, feminists, refugees, and the Canadian Muslim community.

Examples abound relating to the continued and real-life impact of online hate against local Muslim communities. The Fort McMurray Mosque, for instance, has faced numerous threats online for years, including most recently after the New Zealand shootings. Some Facebook users called for the Markaz ul Islam Mosque to be burned down and blown up, while another called for the mosque to "have a pig roast". To our knowledge, while the RCMP did investigate these clear instances of online hate speech, potentially breaching the *Criminal Code*, no charges have been laid.

It is clear, given our current environment, that action must be taken in order to ensure that there is a comprehensive, whole-of-society approach to reducing the harms of online hate.

<sup>&</sup>lt;sup>1</sup> *Maclean's*, "Online hate speech in Canada is up 600 percent. What can be done?", November 2, 2017 (online: Maclean's") <<u>https://www.macleans.ca/politics/online-hate-speech-in-canada-is-up-600-percent-what-can be-done/</u>>.

<sup>&</sup>lt;sup>2</sup> Marian Scott, "Most Canadians have seen hate speech on social media: survey", January 27, 2019 (online: Montreal Gazette) < <u>https://montrealgazette.com/news/local news/hate-speech-targets-muslims</u>>.

<sup>&</sup>lt;sup>3</sup> Barbara Perry & Ryan Scrivens, "A Climate for Hate? An Exploration of the Right-Wing Extremist Landscape in Canada" *Springer- Critical Criminology* 2018, online: https://link.springer.com/article/10.1007%2Fs10612-018-9394-y.

We welcome the work that the federal government is doing to propose an approach to address harmful content online through a new legislative and regulatory framework that would create rules for how social media platforms and other online services must address harmful content. We support an approach that is well-studied, balanced, and constitutional.

#### IV. The Problem: Terrorist Content and Passing Information to Law Enforcment

Examining the discussion guide and technical paper, however, we have serious concerns that undermine our confidence that this framework in its current form would properly balance protecting our democracy and the safety of all Canadians. Our concerns include three key issues:

- The vague and overbroad way that the framework proposes engaging law enforcement and CSIS to address "terrorist content", "terrorist activity", and "terrorism".
- Elements of the framework that would repeat the errors of Bill C-51 "The Anti-Terrorism Act", 2015.
- Elements of the framework that raise risks with regard to the *Canadian Charter of Rights and Freedoms*.

#### III. Engaging law enforcement and CSIS on terrorism

We advise the government to remove all references to "terrorist content", "terrorist activity" and "terrorism" from the approach to address hate and other harmful content online. The purpose of regulating hate online should be to keep all Canadians safe from violence. The track record of the Canadian government's practices with respect to enactment, investigation, enforcement, prosecution, and incarceration around terrorism has disproportionately securitized, criminalized, and demonized Muslim Canadians.

#### The Impugned Provisions

In the Discussion Guide's Module 1, under "Background", the government observes that "Social media platforms can be used to spread hate or terrorist propaganda, counsel offline violence, recruit new adherents to extremist groups, and threaten national security, the rule of law and democratic institutions." Under the section "Who and what would be regulated", the government lists "terrorist content" as the first item in a list of five categories of harmful content.

Under the section on "Engaging law enforcement and CSIS", the government proposes two potential options to achieve the right balance on the mandatory notification requirement, specifically on its scope and the thresholds for triggering notification obligations. The first option refers to illegal content that is "likely to lead to violence or terrorist activity" and the second option proposes that "the threshold for reporting potentially terrorist and violent extremist content" could be lower than that for potentially criminal hate speech".

This could lead to absurd consequences, since a lower threshold than the *Whatcott* standard for "likely to lead to violence or terrorist activity" could mean that Canadian Muslims who talk about Palestine, Afghanistan, or stand in solidarity with diverse movements could be implicated. Clearly, this is unacceptable.

Under the section on "Compliance and enforcement", the government proposes that a Digital Safety Commissioner of Canada would have powers to "apply to the Federal Court to seek an order to require Telecommunications Service Providers to implement a blocking or filtering mechanism to prevent access to all or part of a service in Canada that has repeatedly refused to remove child sexual exploitation and/or terrorist content". We support the government in in implementing this with regard to removal of content that features child sexual exploitation. However, the excessively vague mention of "terrorist content" should be omitted here. It could be replaced with something more specific and clearer like content that "incites to violence".

With regard to the government's Technical Paper that accompanies the Discussion Guide, we also noted very concerning ways of addressing terrorism. In Module 1(A): New legislative and regulatory framework, the government proposes an act of legislation that would be based on several premises. Premise (d) mentions the consideration that Online Communication Services (OCSs) are "used to spread propaganda, recruit, organize and incite violence, and that terrorist content online often leads to violence in the physical world". Reference to "terrorist content online" should be omitted as the objective is achieved clearly by simply relying on the *Whatcott* standard. Under the section on "Application" #8, the government proposes that "The Act should provide definitions for the five (5) types of harmful content according to a set of concepts explained further in that section. The government proposes that legislation "should ensure that the definitions borrow from the Criminal Code but are adapted to the regulatory context." The government goes on to say that "The concept of terrorist content, should refer to content that actively encourages terrorism and which is likely to result in terrorism." This is too vague. The whole sentence starting with "the concept of terrorist content" should be omitted. The way this is proposed puts not only Canadian Muslims at higher risk of harm but also Canadians engaging in political activism around Indigenous rights, anti-Black racism, and climate justice.

Under the section on "Incident response protocol", for #18 [D], the government proposes that legislation should provide the Digital Safety Commissioner with the authority, with the approval of the Governor in Council, to establish an Incident Response Protocol for the purpose of implementing the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online and reducing the online communication of content relating to terrorist activities. The Incident Response Protocol would respond to an act or omission as described in the definition of "terrorist content" tied to an emergent, ongoing, or recently concluded real-world attack in Canada, or outside of Canada when content is shared on one or more Canadian-based OCSs. We suggest that in order to meet our obligations, we need to be clear that we must make our production order protocols more robust.

Reporting and preservation obligations, for #22, the government proposes that for one approach in that section (22 b), legislation should provide that an Online Communication Service Provider (OCSP) shall report information respecting terrorist content and content that incites violence that will be made inaccessible in accordance with this legislation to the Canadian Security Intelligence Service (CSIS) in a manner that conforms to Governor in Council regulations relating to the threshold, timing, format and any other requirements for such reports. Reference to "terrorist content" should be omitted here. If kept, there is an increase in risk to undermining the rule of law and a risk to the privacy rights of Canadians, especially activists, journalists, and others whose content would be at higher risk of erroneous categorization as terrorist content without adequate assessment of context.

Under the section on Exceptional recourse #120, reference to a. II. "terrorist content" should be removed entirely.

V. Elements of the framework that would repeat the errors of Bill C-51 "The Anti-Terrorism Act", 2015.

If this framework is implemented as proposed, we see it as amounting to a new version of Bill C-51 and we would publicly oppose it as such.

Bill C-51 made significant changes to Canada's national security, anti-terrorism, and privacy laws. It treated "terrorism offences" in a vague and overbroad way. This government's proposed framework to address hate online and online harm treats "terrorist content" online in a similarly vague and overbroad way. Due to the massive scale and scope of information, the rapid rate of speed at which content can be generated, modified, and disseminated, the risks and potential harms of this kind of vague and overbroad treatment of terrorist content could be worse than the harms Canadians experienced and/or witnessed from the way previous governments handled "terrorism offences".

Bill C-51 introduced the concept of "terrorist propaganda" into federal legislation and permitted judges to order the removal of such content from the internet. Again, the harms were apparent in attempts to implement such measures by means of people who were not equipped to be aware of and mitigate the harms of unconscious bias at an individual level, nor equipped to address systemic racism at an institutional level. Now this framework would require people working as moderators for social media platforms to also judge what is and what is not "terrorist propaganda" and "terrorist content". For obvious reasons, that is unacceptable. The risks of errors that would have harmful consequences for public safety and our democracy are increasingly high.

As Bill C-51 increased the powers of law enforcement and CSIS, so too does this approach proposed by the government effectively grant law enforcement and CSIS unprecedented access to the user data of Canadians. As Bill C-51 permitted government institutions to share information with each other about "activities that undermine the security of Canada", so too does this framework propose to enable government institutions to share information with each other, except now with digital technologies and the kind of specific granular personal data that was unimaginable before now. What the government is proposing now does not adequately address how to protect Canadians from the risks that such digital data sharing poses to our privacy rights, our freedom of expression, and other democratic freedoms.

Simply put, the legislation as it stands now could inadvertently result in one of the most significant assaults on marginalized and racialized communities in years. NCCM does not participate in hyperbole; but this is gravely, dangerously concerning.

# VI. Elements of the framework that raise risks with regard to the *Canadian Charter of Rights and Freedoms*.

For all the reasons outlined above, it is clear to us that this proposed framework, in its current form, would have a high risk of violating the constitutional rights of Canadians. We are aware of other stakeholders who also see the risks this framework poses for Charter violations. If this framework is implemented as proposed, the NCCM is prepared to collaborate with other stakeholders nationally and across sectors to challenge the constitutionality of this approach to address online hate.

There is a strong likelihood that these provisions of the frameworks – that amount to one of the largest information gathering provisions in recent history to national security agencies in a way that seems to completely lack transparency - may violate section 8 of the Charter, amongst other sections of the Charter.

#### **VII.** Conclusion

While the NCCM supports more online hate regulation, we do not support regulation that can be used to harm the safety of Canadian Muslims and other securitized groups, to undermine the healthy flourishing of active digital citizenship, or that be used to harm the fundamental democratic freedoms of all Canadians.

Dissummed commonity of a series in la Ego due l'annés d'Dullarmalian Ducturier il inferenzi due quine fit ille luccase la constantante acti





## Impacts of criminalization and punitive regulation of online spaces: The need for sex workers' voices

## A Submission to the Digital Citizen Initiative, Department of Canadian Heritage

RE: The Government's proposed approach to address harmful content online

Jennie Pearson

Graduate Research Assistant and Community Engagement Associate |AESHA Project PhD Student |Interdisciplinary Studies Graduate Program at the University of British Columbia

Andrea Krüsi, PhD Research Scientist | Centre for Gender and Sexual Health Equity Assistant Professor | Department of Medicine at the University of British Columbia

Shira Goldenberg, PhD Director of Research Education | Centre for Gender & Sexual Health Equity Assistant Professor | School of Medicine, SUC an Diego

> Raji Mangat Executive Director | West Coast LEAF Association

Sharnelle Jenkins-Thompson Manager of Community Outreach | West Coast LEAF Association

#### **Our Position:**

We at the Centre for Gender and Sexual Health Equity (CGSHE) and West Coast LEAF share the concern of the Digital Citizen Initiative about the impact of harmful content online, including the sharing of non- consensual sexual content. However, we are concerned that further punitive regulation and the introduction of new regulations and enforcement mechanisms to govern user activity online will have broad negative consequences for communities already heavily regulated and surveilled in the online sphere, including sex workers. Sex workers are experts in the negotiation of consent and in safely navigating sexually explicit materials online, therefore sex workers and considerations about their occupational health and safety must be included in deliberations about policy responses to harmful content online.

As outlined below, a significant body of peer-reviewed empirical evidence on sex work policy unequivocally demonstrates that punitive and restrictive regulations and policies undermine sex workers' occupational health and safety and push sex work underground. Indeed, regulatory models based on surveillance and criminalization have previously been shown as ineffective in curbing exploitation, and are instead shown to undermine sex workers' ability to access vital occupational health and safety protections (1-2). Digital environments have been identified as critical to sex workers' safety and autonomy (13-17). Deliberations about how to respond to online harms that fail to include or address sex workers' realities have the potential to create serious negative effects to sex workers' occupational health and safety and at the same time, are unlikely to reach the stated goals of preventing online harms (including non-consensual sharing of sexual content) (1-2). Through West Coast LEAF's ongoing monitoring of the gender-based impact of COVID- 19, the importance of digital environments for sex workers has only increased as many sex workers have had to pivot to or continue working online to support their economic and health and safety needs in the face of financial devastation unrecognized by the financial supports rolled out by federal or provincial governments (3).

#### The Research:

#### **Recent Science & Policy Developments:**

Empirical evidence has consistently highlighted that criminalization, policing and punitive regulation are the key drivers that continue to undermine sex workers' human and labour rights, including occupational health and safety (4-6). In 2013, the Supreme Court of Canada (SCC) ruled unanimously in Canada (Attorney General) v Bedford, 2013 SCC 72 that the criminalization of sex work under previous legislation was unconstitutional, however new aspects of sex work were criminalized under the new "end-demand" laws implemented in 2014. Qualitative and epidemiological research shows that current end-demand sex work laws reproduce harms to workers, including increased violence and barriers to accessing justice and health and labour protections (7-12).

Further punitive restrictions and avenues of enforcement to regulate online sex work have the potential to compromise digital work environments that have been shown to afford additional safety for sex workers (13-17). Online sex work and solicitation can be a safe(r) environment for workers

when compared to street-based sex work and serves as a critical livelihood for many workers in the sex industry. In a context where most aspects of sex work are already criminalized, but where selling sex itself is legal per new end-demand laws, it is imperative that sex workers' occupational health and safety is considered when deliberating about online harms in spaces sex workers use, including sites such as Pornhub. To avoid further jeopardy to the online workplaces of sex workers, sex workers themselves must be consulted on decisions about how to organize websites that host sexually explicit content. Indeed, sex workers are experts and can provide important insights on protection of privacy and consent. Moreover, proactively hearing from and responding to the concerns of sex workers on the very issues that impact their lives and livelihoods is essential to promoting access to justice for this population, recognized as facing particular stigma and challenges in accessing legal remedies and safe workspaces (18,19) (see also, Canada (Attorney General) v Downtown Eastside Sex Workers United Against Violence Society, 2012 SCC 45 (20))

#### The evidence on punitive approaches to sex work

AESHA is a 10-year longitudinal community-based research project housed at the University of British Columbia and Simon Fraser University-affiliated CGSHE, that includes over 900 sex workers across diverse work environments. AESHA research adds to the growing body of evidence globally that highlights how the current approaches criminalizing sex work and punitive regulation and censorship of sexually explicit material harm sex workers by increasing risk of violence, jeopardizing occupational health and safety, and reducing income security.

• Harms of sex work criminalization. AESHA's research has highlighted the pivotal role of criminalization, policing and surveillance in shaping the health, safety and human rights of sex workers (7-10-9). Criminalization and policing disproportionately impact marginalized populations of sex workers, including racialized and Indigenous, im/migrant workers, trans sex workers and sex workers who use drugs (9-12), and are often determined by the socio-spatial features of sex work venues and locations (21-23). Canada's end demand laws perpetuate existing harms for sex workers, including elevated risk of violence, barriers to accessing justice and continued stigma and fear that prevent access to safe, secure housing, healthcare, and social protections (24-28). These harms disproportionately impact racialized, im/migrant sex workers, who are viewed categorically as victims of exploitation, but at the same time deemed unworthy of occupational protections (24-30).

• Online access is necessary for sex workers' safety, autonomy, and security. Digital tools used for solicitation, content distribution, client communication and violence reporting support sex workers' occupational safety, by allowing for improved client screening, increased control and worker autonomy (13-15). Online censorship policies, punitive laws and increased surveillance and enforcement jeopardize sex workers' access to these occupational health and safety strategies. Rather than increased punitive regulation, AESHA's research demonstrates the need to remove barriers to access online spaces for sex work and greater access to digital technologies.

• Decriminalization, not heightened punitive regulation and enforcement, is necessary to root out exploitation. As outlined by Canada's Justice Minster in a recent statement, the Criminal Code already includes sections specifically prohibiting the publishing and/or selling of sexually explicit material relating to children in a comprehensive way (section 163.1 child pornography), as well as voyeurism and the non-consensual distribution of intimate images, (sections 162, 162.1, 163) (29). Recommendations for more broad, punitive regulation which may conflate child pornography and non-consensual materials with sex work, in turn, work to undermine online sex workspaces. Additional regulation and censorship of online spaces where sex workers operate will further hinder sex workers' occupational health and safety and is more likely to foster exploitation by pushing sex work further 'underground'. The evidence shows that decriminalization, and sex worker-led harm reduction strategies, rather than regulation or punitive approaches, are most effective in addressing trafficking, exploitation and violence in the context of sex work (30-32)

#### **Policy Implications:**

Despite being frequently positioned as serving to protect women and survivors of non-consensual content distributions, AESHA's findings indicate that the current broad discussion to further regulate online spaces fuels stigma against sex workers and violates sex workers' human rights by exacerbating risk for sex workers and communities already vulnerable to violence and exploitation.

In other jurisdictions, such as the United States, further criminalization and regulation of online sexually explicit content has been found to be ineffective in discouraging non-consensual distribution or sexual violence but has proved to harm sex workers and pushed the industry further underground and outside the parameters of safe(r) online spaces (16, 17, 33). Punitive regulation of online spaces and sexually explicit content has resulted in broad censorship policies that remove content belonging to sex workers. In line with the recommendations made by international policy bodies such as the World Health Organization, UNAIDS and Amnesty International (34-36), the above outlined peerreviewed empirical evidence demonstrate the negative impacts of criminalization and punitive regulation on sex workers' occupational health and safety.

We urge the Digital Citizen Imitative to consider the above outlined empirical evidence in their deliberations and make an evidence-based call to:

 meaningfully consult with sex workers in any deliberations about online sexually explicit content

 refrain from implementing further punitive restrictions that may impact online sex work environments.

#### About the AESHA Project at the CGSHE:

The Centre for Gender and Sexual Health Equity's Assessment of Sex Workers' Health Access (AESHA) Project is a 10-year longitudinal community-based research project that includes a quantitative cohort and qualitative/ethnographic arm. The CGSHE is a University of British Columbia and Simon Fraser University-affiliated research centre at Providence Health Care. As part of the quantitative arm, AESHA operates a community-based prospective cohort of over 900 sex workers across diverse work environments. The qualitative arm is focused on documenting the lived experiences of sex workers of all genders, and third parties who provide services for sex workers (e.g., receptionists, venue managers, owners and security personnel). Over the past 5 years, the AESHA project focused on evaluating the impact of evolving legislative approaches to the regulation of sex work including the Canadian 'end-demand' laws (The Protection of Exploited Persons and Communities Act) on sex workers' health, safety, and human rights.

This research has been shared in 38 peer-reviewed articles and a recent report on the harms of enddemand legislation, which our team submitted to the federal Department of Justice and all MPs and Senators. Our team also leveraged AESHA findings in a submission to the Committee on the Elimination of Discrimination Against Women (CEDAW) of the United Nations Office of the High Commissioner on Human Rights calling for an end of the conflation between sex work and sex trafficking. AESHA is built on partnerships with SWUAV, SWAN, PACE, WISH, HIM/HUSTLE, Pivot, Canadian HIV/AIDS Legal Network, and the BCCDC. The Centre for Gender and Sexual Health Equity (CGSHE) has a strategic mandate to advance gender & sexual health equity among marginalized populations in BC, Canada, and globally through three pillars: research, policy, and practice. These pillars incorporate community-based, clinical and population health research, policy evaluation, implementation science and education.

#### About West Coast LEAF:

West Coast LEAF is dedicated to using the law as a strategy to work towards an equal and just society for all women and people who experience gender-based discrimination. Since our founding in 1985, we have helped bring about some of Canada's most important feminist victories for reproductive rights, workplace standards, fairness in family law, legal protections from sexual harassment, and more. In collaboration with community, West Coast LEAF uses litigation, law reform, and public legal education strategies to create social change. While we are focused on issues in British Columbia, we also take action in matters of national significance that are important to the equality and human rights of people in British Columbia. We aim to transform society by achieving access to healthcare; access to justice; economic security; freedom from gender-based violence; justice for those who are criminalized; and the right to parent.

#### Acknowledgements:

CGSHE thanks all those who contributed their time and expertise to the AESHA Project, particularly research participants, AESHA community advisory board members and partner agencies, and the

AESHA team, including: Kate Lumsdon, Alka Murphy, Jennifer McDermid, Jennifer Morris, Shannon Bundock, Sylvia Machat, Tina Beaulieu, Christie Ngozi Gabriel, Natasha Feuchuk, Lois Luo, Minshu Mo, Sherry Wu, Zoe Hassall, Emma Kuntz, Bronwyn McBride, and Sarah Moreheart. We also thank Melissa Braschel, Peter Vann, Megan Bobetsis and Arveen Kaur for their research and administrative support.

West Coast LEAF would like to thank our community partners who have supported on BC Gender Equality Report Card and have informed our ongoing learning about the needs of sex workers pre- and during this pandemic. Thank you to PACE Society, the Coalition Against Trans Antagonism and the UNYA Native Youth Learning Centre and 2-Spirit Collective.

#### References

1. Global Network of Sex Work Projects (2018). The Impact of Anti-trafficking Legislation and Initiatives on Sex Workers. https://www.nswp.org/sites/nswp.org/files/impact\_of\_anti-

trafficking\_laws\_pb\_nswp\_-\_2018.pdf

United Nations Development Programme, 2012, "HIV and the Law: Rights, Risks, and Health," 39–40.
 West Coast LEAF (2020). COVID-19 BC Gender Equality Report Card.

http://www.westcoastleaf.org/wp- content/uploads/2020/12/West-Coast-LEAF-COVID-report-card-Dec-7-web-final.pdf

4. Platt, L., Grenfell, P., Meiksin, R., Elmes, J., Sherman, S. G., Sanders, T., ... & Crago, A. L. (2018). Associations between sex work laws and sex workers' health: A systematic review and meta-analysis of quantitative and qualitative studies. PLoS medicine, 15(12), e1002680.

 Crago, A. L., Bruckert, C., Braschel, M., & Shannon, K. (2021). Sex Workers' Access to Police Assistance in Safety Emergencies and Means of Escape from Situations of Violence and Confinement under an "End Demand" Criminalization Model: A Five City Study in Canada. Social Sciences, 10(1), 13.
 Parliament of Canada . 2014. C-36 (41-2) - Royal Assent - Protection of Communities and Exploited Persons

Act . Ottawa: Parliament of Canada. http://www.parl.ca/DocumentViewer/en/41-2/bill/C-36/royalassent/page-33#3

7. Krüsi A, Chettiar J, Ridgway A, Abbott J, Strathdee SA, Shannon K. Negotiating safety and sexual risk reduction with clients in unsanctioned safer indoor sex work environments: a qualitative study. Am J Public Health. 2012;102(6):1154-9

8. Krüsi A, Kerr T, Taylor C, Rhodes T, Shannon K. 'They won't change it back in their heads that we're trash': the intersection of sex work-related stigma and evolving policing strategies. Sociology of health & illness. 2016.

9. Krüsi A, Pacey K, Bird L, Taylor C, Chettiar J, Allan S, et al. Criminalisation of clients: reproducing vulnerabilities for violence and poor health among street-based sex workers in Canada: a qualitative study. BMJ Open. 2014;4(6):e005191.

10. Lyons T, Krüsi A, Pierre L, Kerr T, Small W, Shannon K. Negotiating Violence in the Context of Transphobia and Criminalization The Experiences of Trans Sex Workers in Vancouver, Canada. Qualitative health research. 2015:1049732315613311.

11. Shannon K, Strathdee SA, Shoveller J, Rusch M, Kerr T, Tyndall MW. Structural and environmental barriers to condom use negotiation with clients among female sex workers: implications for HIV-prevention strategies and policy. Am J Public Health. 2009;99(4):659-65.

12. AESHA Project. Harms of End-Demand Criminalization: Impact of Canada's PCEPA Laws on Sex Workers' Safety, Health & Human Rights (2019).

http://www.cgshe.ca/app/uploads/2019/12/Harms\_2019.12.16.v1.pdf

13. Machat, S et al. Internet solicitation linked to enhanced occupational safety outcomes for sex workers in Metro Vancouver: 2010-2018. In review.

14. Argento E, Taylor M, Jollimore J, et al. The Loss of Boystown and Transition to Online Sex Work: Strategies and Barriers to Increase Safety Among Men Sex Workers and Clients of Men. American Journal of Men's Health. November 2018:1994-2005. 15. Scoular, J., Pitcher, J., Sanders, T., Campbell, R. and Cunningham, S. (2019), Beyond the Gaze and Well Beyond Wolfenden: The Practices and Rationalities of Regulating and Policing Sex Work in the Digital Age. Journal of Law and Society, 46: 211-23

16. Blunt , D. and Wolf, A. 'Erased: The impact of FOSTA-SESTA and the removal of Backpage on sex workers', Anti-Trafficking Review, issue 14, 2020, pp. 117-121,

https://doi.org/10.14197/atr.201220148

17. Blunt, D., Wolf, A., Coombes, E., Mullin, S. Posting into the void: Studying the impact of shadow banning on sex workers and activists (2020).

18. Krüsi A, Kerr T, Taylor C, Rhodes T, Shannon K. 'They won't change it back in their heads that we're trash': the intersection of sex work-related stigma and evolving policing strategies. Sociology of health & illness. 2016 Sep;38(7):1137-50.

19. McBride B, Shannon K, Bingham B, Braschel M, Strathdee S, Goldenberg SM. Underreporting of Violence to Police among Women Sex Workers in Canada: Amplified Inequities for Im/migrant and In-Call Workers Prior to and Following End-Demand Legislation. Health Hum Rights. 2020 Dec;22(2):257-270. PMID: 33390711; PMCID: PMC7762889.

20. Canada (Attorney General) v Downtown Eastside Sex Workers United Against Violence Society, 2012 SCC 45, available: https://scc-csc.lexum.com/scc-csc/scc-csc/en/10006/1/document.do.

21. Anderson S, Xi Jia, Liu V., Chattier, J., Krüsi, A., Allan, S., Maher, L., Shannon, K. Violence Prevention and Municipal Licensing of Indoor Sex Work Venues in the Greater Vancouver Area: Narratives of Migrant Sex Workers, Managers and Business Owners. Culture Health & Sexuality. 2015.

22. Goldenberg SM. Trafficking, migration, and health: complexities and future directions. The Lancet Global Health. 2015;3(3):e118-e9.

23. Anderson S, Shannon K, Li J, Lee Y, Chettiar J, Goldenberg S, et al. Condoms and sexual health education as evidence: impact of criminalization of in-call venues and managers on migrant sex workers access to HIV/STI prevention in a Canadian setting. BMC International Health and Human Rights. 2016;16(1):30.

24. Argento E GS, Braschel M, Machat S, Strathdee S, Shannon K. The impact of end-demand legislation on sex workers' access to health and sex worker support services: A community-based prospective cohort study in Canada. PLoS One. 2020 Apr 6;15(4)

25. Machat S SK, Braschel M, Moreheart S, Goldenberg S. Sex Workers' experiences and occupational conditions post- implementation of end-demand criminalization in Metro Vancouver, Canada. Canadian Journal of Public Health. 110(5):575-583.

26. McBride B, Goldenberg SM, Murphy A, Wu S, Braschel M, Krüsi A, Shannon K. Third Parties (Venue Owners, Managers, Security, etc.) and Access to Occupational Health and Safety Among Sex Workers in a Canadian Setting: 2010-2016. American Journal of Public Health. 2019 May; 109(5): 792-798.

27. McBride B, Shannon K, Duff P, Mo M, Braschel M, Goldenberg SM. (2019). Harms of Workplace Inspections for Im/ Migrant Sex Workers in In-Call Establishments: Enhanced Barriers to Health Access in a Canadian Setting. Journal of Immigrant and Minority Health. 21(6):1290-1299.

28. McBride B, Shannon K, Murphy A, Wu S, Erickson M, Goldenberg SM, Krüsi A. Harms of third party criminalisation under end-demand legislation: undermining sex workers' safety and rights Culture, Health & Sexuality. 2020 Aug; 22(9).

29. Secretariat, Treasury Board of Canada. "Question Period Note Details - Illegal Online Content and Canada's International Trade Obligations - Jus, JUS-2020-QP-00005." Accessed March 9, 2021. https://search.open.canada.ca/en/qp/id/jus, JUS-2020-QP-00005. 30. Goldenberg, Shira M. "Trafficking, Migration, and Health: Complexities and Future Directions." The Lancet Global Health 3, no. 3 (March 1, 2015): e118–19. https://doi.org/10.1016/S2214-109X(15)70082-3

31. Steen, Richard, Smarajit Jana, Sushena Reza-Paul, and Marlise Richter. "Trafficking, Sex Work, and HIV: Efforts to Resolve Conflicts." The Lancet 385, no. 9963 (January 10, 2015): 94–96. https://doi.org/10.1016/S0140- 6736(14)60966-1.

32. Rekart, Michael L. "Sex-Work Harm Reduction." The Lancet 366, no. 9503 (December 17, 2005): 2123-34. https:// doi.org/10.1016/S0140-6736(05)67732-X.

33. Morgan, E. "On Fosta and the Failures of Punitive Speech Restrictions." Northwestern University Law Review 115, no. 2 (September 2020): 503–47.

34. World Health Organisation (WHO). Consolidated guidelines on HIV prevention, diagnosis, treatment and care for

key populations. Geneva: World Health Organisation; 2014

35. UNAIDS (2014) The Gap Report: Sex Workers.

www.unaids.org/en/resources/documents/2014/Sexworkers

36. Amnesty International. Sex Worker's Rights are Human Rights. 2015.

https://www.amnesty.org/en/latest news/2015/08/sex-workers-rights-are-human-rights

## **INDEPENDENT PRESS GALLERY**

BY EMAIL (pch.icn-dci.pch@canada.ca)

September 24, 2021

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy Street Gatineau, QC K1A 0S5

Dear Digital Citizen Initiative:

#### Re: Harmful Online Content Feedback

I am the President of the Independent Press Gallery of Canada ("**IPG**"). This letter is provided as feedback on the Government of Canada's proposed approach to regulating social media and harmful online content. We hope you take our perspectives seriously in crafting any bill the Government may intend to introduce on this topic.

Generally, we assert that the proposed approach desperately needs to be reconsidered, with greater consultation and further analysis taking place before proceeding. The proposal has significant legal issues throughout and harmful legal consequences to *Charter*-protected freedoms and the rule of law.

The IPG is a not-for-profit dedicated to the promotion of a free and independent media in Canada. We have a large membership, which includes independent journalists and media outlets. We support and advocate for a media that remains separate from the government, and have a strong commitment to *Charter* values, particularly freedom of expression, association, and free press. The IPG is vital to the fabric of Canada and essential to an independent media. The Government regulation, as proposed, is detrimental to these democratic values.

Sense and a sense of the provident of the sense the sense of the sense

In preparing these comments we have reviewed several sources. The following is an outline of our response.

- Bill C-36

   The Definition of Hatred
   Discrimination by Hate Speech

   Discussion Guide and Technical Paper

   Module 1: Regulating Social Media
   Hate Speech
   Freedom of Expression
   Other Harms and Delegation of Authority
   Suspicions and Bias
   No Justification
  - Module 2: Modifying the Legal Framework Privacy Issues
- 3. Conclusion

#### 1. Bill C-36

The Discussion Guide starts out by referring the reader to Bill C-36, which was introduced on June 23, 2021. The Discussion Guide advises that Bill C-36 will "complement the regulatory approach for online social media platforms." The Technical Paper mentions hate speech in one paragraph<sup>1</sup> out of 126, so by inference, Bill C-36 is instrumental in understanding the regulation of social media and harmful online content.

#### The Definition of Hatred

Bill C-36 introduces a new defined term, "hatred", into the *Criminal Code*, which is particularly concerning for being vague, ambiguous, and difficult (if not impossible) to distinguish where dislike or disdain end and hatred begin:

*hatred* means the emotion that involves detestation or vilification and that is stronger than dislike or disdain; (haine)

<sup>&</sup>lt;sup>1</sup> Technical Paper, paragraph 8.

ten standardar esta statistica positica (o cartos) los que a positica de la Sura de Glavina do sur la comunicada a disconsidor españolamente de esta comunicada cartos de la cartos de esta comunicada comunicada comunicada

The Supreme Court of Canada, and Courts across the country have struggled with the interpretation and application of section 319 of the *Criminal Code* for the public incitement of hatred. It is not an easy concept to define, and it is not something tangible that we can all agree has occurred or has not. It is nuanced, and is usually informed by a person's own experiences and philosophies. Hatred, according to the Courts, is separate from violence and threats of violence. Hatred is, as it is put in the definition in Bill C-36, an emotion, a personal and subjective experience. The problem with criminalizing such an emotion was put succinctly by Justice McLachlin (as she was then):

It is not only the breadth of the term "hatred" which presents dangers; it is its subjectivity. "Hatred" is proved by inference -- the inference of the jury or the judge who sits as trier of fact -- and inferences are more likely to be drawn when the speech is unpopular. The subjective and emotional nature of the concept of promoting hatred compounds the difficulty of ensuring that only cases meriting prosecution are pursued and that only those whose conduct is calculated to dissolve the social bonds of society are convicted.<sup>2</sup>

The definition proposed in Bill C-36 does nothing to clarify when an emotion becomes criminal.

Currently, Canada is amid a pandemic. Vaccination mandates are being rolled out by provincial, municipal, and federal governments, as well as businesses and all sorts of employers. Those who support these efforts detest and vilify those who object to vaccination or oppose the mandates. Emotions are high on both sides, are politicized and are polarizing. Certainly, the vaccinated and unvaccinated are identifiable groups for the purposes of section 319(2) of the *Criminal Code* - we have government issued identification papers to distinguish one group from the other, as well as different applicable criteria and accessibility between the groups. This current climate is a perfect example as to the problem with this definition and the criminalization of hatred - none of the defences listed in section 319(3) of the *Criminal Code* would immunize comments of detestation or vilification directed towards either group. Such politicized positions as between interests respecting bodily autonomy and public health, should <u>not</u> attract criminal liability. To legislate such a definition of hatred, in the way proposed, is

<sup>&</sup>lt;sup>2</sup> R v Keegstra, [1990] 3 SCR 697 at 856 (McLachlin J, dissent).

to encourage the difficulties identified by our former Chief Justice rather than mitigate those difficulties.

#### Discrimination by Hate Speech

Bill C-36 also proposes to create a new category of discrimination in the *Canadian Human Rights Act*, RSC 1985, c H-6 ("*CHRA*"), the expression of hate speech on the internet or by other means of telecommunication. This is nonsensical, in that it proposes to regulate online communications for hate speech but provides no recourse to verbalized hate speech. This two-tiered system of communication is problematic. In addition, the definition of hate speech faces the same problems that the definition of hatred faces. It is a nearly impossible to get a uniformed appreciation as to what is, or is not, hate speech.

The exemption to hate speech, as set out in proposed section 13(5), fails to understand the nuance of online communication:

#### Exception — private communication

(5) This section does not apply in respect of a private communication.

There is no guidance in this Bill or in the proposed revisions to the CHRA to determine when a communication is private. There are several online communications that one may consider private or public, such as communications posted to a private group, direct messages, group messages, posts by a private account, posts where only a handful of people have seen the communication or could see the communication. Then the question arises of who is responsible for the private communication when it is made public by screen shot or shared to a wider, more public audience. Section 13(3)(a) seems to protect someone who amplifies the communication, leaving an unintelligible structure to monitor online communication. Bill C-36 is woefully disconnected to the manner of communications online.

Accepting section 13 as it is, it is also difficult to establish how "online hate speech" can be discriminatory. There is a standard test for discrimination:

- 1. Does the complainant have a protected characteristic?
  - a. In the CHRA, protected characteristics are race, national or ethnic origin, colour, religion, age, sex (including pregnancy or child-

birth<sup>3</sup>), sexual orientation, gender identity or expression, marital status, family status, genetic characteristics (including a refusal to undergo genetic testing or disclose results of such testing<sup>4</sup>), disability and conviction for an offence for which a pardon has been granted or in respect of which a record suspension has been ordered.<sup>5</sup>

- 2. Did the complainant suffer an adverse consequence?
  - a. In the CHRA the adverse consequence must be related to the access of goods, services, facilities, or accommodations;<sup>6</sup> residential accommodation;<sup>7</sup> employment, employment organizations, employment policies, wages, or employment applications and advertisements;<sup>8</sup> or the publication of notices, signs, symbols, emblems.<sup>9</sup>
- 3. The adverse consequence must be related to the protected characteristic.<sup>10</sup>

This three-part test is commonly referred to as the *Moore* test. In the *CHRA* it is also discriminatory when a person is harassed on the basis of a protected characteristic in the provision of goods and services, commercial or residential accommodation, or in matters related to employment.<sup>11</sup> It would have made far more sense to craft a hate speech section that mirrored section 14 of the *CHRA* on harassment, to confine alleged discrimination to the usual boundaries of protected grounds and specific adverse effects. As it is currently drafted in Bill

<sup>3</sup> CHRA, s 3(2).

- 5 CHRA, s 3(1).
- 6 CHRA, s 5
- 7 CHRA, s 6
- 8 CHRA, s 7-11
- 9 CHRA, s 12

10 Moore v British Columbia (Education), 2012 SCC 61 at para 33.

11 CHRA, s 14

<sup>4</sup> CHRA, s 3(3).

C-36, the Canadian Human Rights Commission will be inundated with allegations of hate speech where the speech is of a quasi-private nature, or the complainant has not suffered an adverse consequence in the protected areas as required by part two of the *Moore* test. Finally, it is arbitrary, unreasonable, overly broad, and unnecessary for the Commission to have jurisdiction over communication on the internet or by telecommunication, where the same communication made verbally or in print would fall outside the Commission's jurisdiction.

Concerningly, Bill C-36 leaves anyone open to accusation of hate speech, with little recourse in which to make a reasonable response or defence. This is made clear by the proposed section 40(8):

The Commission may deal with a complaint in relation to a discriminatory practice described in section 13 without disclosing, to the person against whom the complaint was filed or to any other person, the identity of the alleged victim, the individual or group of individuals who has filed the complaint or any individual who has given evidence or assisted the Commission in any way in dealing with the complaint, if the Commission considers that there is a real and substantial risk that any of those individuals will be subjected to threats, intimidation or discrimination.

The proposed section 40(8) is contrary to the rule of law and runs afoul the principles prescribed in section 11(a) of the *Charter*.

In sum, Bill C-36 is a poor foundation upon which to build a regulatory structure for social media and harmful online content.

#### 2. Discussion Guide and Technical Paper

Collectively, we have referred to the Discussion Guide and Technical Paper as the "**Proposal**" throughout the remainder of these feedback submissions.

#### Module 1: Regulating Social Media

There are five categories of harmful content enumerated in the Proposal. Our comments will focus on three categories:

terrorist content;

- content that incites violence; and
- hate speech.

These categories are tied to freedoms of expression and the IPG has serious concerns about the proposed regulation of these categories, as will be described in further detail below.

### Hate Speech

The hate speech category is presumably informed by Bill C-36. The Proposal suggests that hate speech "should only be considered as harmful content for the purpose of the Act when communicated in a context in which it is likely to cause harms identified by the Supreme Court of Canada and in a manner identified by the Court in its hate speech jurisprudence."<sup>12</sup> This is wholly unclear and ambiguous. What harms identified by the Supreme Court? What case? Are these harms identified in the criminal law, Canadian human rights law, regulatory law, or civil law context? On what balance of proof should the likelihood of these harms be considered? This paragraph refers to the amended *CHRA*, which (i) has not yet been amended, (ii) has no case law associated to hate speech provisions, and (iii) does not otherwise have hate speech provisions in the unamended version. As a result, it is difficult to understand what "harms identified by the Supreme Court of Canada" could be contemplated in the application of the Proposal. This ambiguity causes the IPG serious concerns.

### Freedom of Expression

Although the Proposal alleges that it regulates Online Communications Services Providers ("**OCSP**"), the result is the indirect regulation and suppression of *users* who post content to those sites. The Proposal infringes on those users' freedom of expression and creates an unreasonable censorship mechanism.

OCSP who cooperate with the regulatory structure will be motivated to respond overzealously to avoid unnecessary business risks. This risk aversion has been identified extensively in public commentary on the Proposal. OCSP will engage in censorship to avoid investigation, shutdowns, and disproportionate fines. Again, this censorship will have extensive impacts on freedom of expression. These

<sup>12</sup> Technical Paper at para 8.

impacts do not meet the requirements for *Charter*-infringing legislation to ensure minimal impairment and proportionality to objectives.

Finally, the "exceptional recourse"<sup>13</sup> power to block sites from use in Canada for persistent non-compliance is an egregious and disproportionate exercise of government authority, particularly if such commonplace and integral sites such as YouTube or Twitter were suddenly blocked from use or access by Canadians. To block a whole site, which contains extensive relevant and necessary content that is not harmful, in response to non-compliance regarding a small portion of the content available, is undemocratic.

#### Other Harms and Delegation of Authority

In addition to the categories identified, the Discussion Guide also notes that, "the Government recognizes that there are other online harms that could also be examined and possibly addressed through future programming activities or legislative action." The Technical Paper alludes to types and subtypes of harmful content as well.<sup>14</sup> Such statements are concerning. It is unclear from the Proposal upon which basis "other harms" will be identified or brought into this regulatory framework. The main concern being that the legislation will be drafted to subdelegate such authority to a Minister or the Governor in Council to prescribe "other harms".

We expect that Parliament may subdelegate the authority to prescribe "other harms" by regulation. Although the British Columbia Court of Appeal observed that "the case law on delegation of legislative powers admits of few, if any restrictions, on the scope or content of what powers may constitutionally be delegated,"<sup>15</sup> this does not mean that this is the type of regulatory authority that should be delegated to the Governor in Council. It is more appropriate to delegate authority for public convenience and general policies,<sup>16</sup> rather than delegating authority which will almost certainly have a direct effect on *Charter* rights. The Governor in Council is the executive branch of the government, has

<sup>13</sup> Technical Paper at paras 120-123.

<sup>14</sup> Technical Paper at para 11(c).

<sup>15</sup> Sga'nism Sim'augit (Chief Mountain) v Canada (Attorney General), 2013 BCCA 49 at para 89.

<sup>&</sup>lt;sup>16</sup> Portnov v Canada (Attorney General), 2021 FCA 171 at para 21, citing Thorne's Hardware Ltd v The Queen, [1981] 1 SCR 106 at 111.

no opposition, and has no specialized knowledge regarding when or whether certain content is harmful. Generally, we submit that the sub-delegation of legislative powers is undemocratic in that executive action is ordinarily exercised without due process, procedural fairness, or consultation, is often politicized, does not reflect the will of the populace, fails to achieve the transparency, and is usually not subject to the review that parliamentary legislation is subjected to. The Governor in Council should only be granted authority that is broad, generalized, and "commonplace"<sup>17</sup> for the purpose of generalized management of government or policy determinations. The Governor in Council should not receive broad authority which relies on a subjective opinion which will invariably infringe on the freedom of expression.

Undefined "other harms", such as harassment, privacy violations, or defamation, would be even more difficult for OCSP to monitor, than the harms explicitly identified in the Proposal. As has been noted by many commentators, the Proposal is likely to result in responses by OCSP that favour risk aversion over freedom of expression. These risks to *Charter*-protected rights will be amplified if the Governor in Council is granted regulation making authority to broaden the scope "harmful content". The risk aversion outcome is amplified by the obligation imposed on an OCSP to remove harmful content within 24 hours of being flagged<sup>18</sup> and the excessive administrative monetary penalties which are not proportional to the supposed harms.<sup>19</sup>

The Technical Paper contemplates a very vague and possibly very broad delegation of authority to the Governor in Council,<sup>20</sup> many areas of contemplated delegations of authority,<sup>21</sup> and further subdelegation by the Governor in Council to the Digital Safety Commissioner.<sup>22</sup> This delegation of authority is problematic for all the reasons listed above: transparency, justification, judicial review, and procedural fairness. As a constitution academic, Lorne Neudorf said:

<sup>&</sup>lt;sup>17</sup> Patrick Monahan, Byron Shaw & Padraic Ryan, Constitutional Law, 5th ed (Toronto: Irwin Law Inc, 2017) at 57-58.

<sup>&</sup>lt;sup>18</sup> Technical Paper at para 11(a), 12(b).

<sup>&</sup>lt;sup>19</sup> Technical Paper at paras 108, 119.

<sup>&</sup>lt;sup>20</sup> Technical Paper at para 5.

<sup>&</sup>lt;sup>21</sup> Technical Paper at paras 3, 9, 11

<sup>22</sup> Technical Paper at paras 10, 12.

ten start och er stort för förstart i svart so Sa gen av en av som stort förförard som Konstanda för det som konstandet som Hendere Stör som för tandet som

Under the Constitution of Canada, Parliament is placed firmly at the centre of public policymaking by being vested with exclusive legislative authority in certain subject matters. Parliament must therefore play the principal federal lawmaking role. The Supreme Court's 1918 judgment<sup>[23]</sup> should no longer be followed to the extent that it allows courts to accept near unlimited delegation of Parliament's lawmaking powers to the executive. [...] Courts and Parliament must take delegation more seriously, and constitutional safeguards should be established to better protect the role of Parliament as lawmaker in chief and restore the proper constitutional balance.<sup>24</sup>

The IPG agrees with Mr. Neudorf's comments. The delegation to the executive in the Proposal is so extensive that it is unconstitutional and contrary to the balance of powers.

#### Suspicions and Bias

We also raise issues with the obligation on OCSPs to make reports to the RCMP when they have "reasonable grounds to suspect" harm. First, this Proposal is supposed to be a regulatory process, and not an expansion of policing obligations to private organizations. Second, unbridled and discretionary authority based on suspicions will almost certainly result in disproportionate policing (by OCSP and law enforcement) of racialized and low-income communities,<sup>25</sup> as well as those who express unpopular speech.

#### No Justification

The Proposal is overly broad and unworkable. It encroaches on free expression and fails to provide adequate protection to ensure that the Executive or regulator exercise their authority reasonably. The mechanisms and results proposed will stifle communication, infringe on basic freedoms, and suppress diversity of perspectives. The Proposal will also unjustifiably violate privacy interests, and likely result in discriminatory policing. The fact that the Proposal is silent on

<sup>23</sup> A reference to Re: Gray, (1918) SCR 150, 42 DLR 1.

<sup>&</sup>lt;sup>24</sup> Lorne Neudorf, "Reassessing the Constitutional Foundation of Delegated Legislation in Canada" (2018) 41:2 Dal LJ 519 at 519.

<sup>25</sup> R v Le, 2019 SCC 34 at para 97.

safeguards for freedom of expression or consideration of *Charter* rights is alarming and leaves the impression that the Government has either failed to consider *Charter*-protected freedoms or has no interest in ensuring that the violations are justifiable.

We remind the Government that it **must** show that legislation which violates *Charter*-protected rights and freedoms is justified:

Canada must show that the law has a pressing and substantial object and that the means chosen are proportional to that object. A law is proportionate if (1) the means adopted are rationally connected to that objective; (2) it is minimally impairing of the right in question; and (3) there is proportionality between the deleterious and salutary effects of the law.<sup>26</sup>

There is nothing in the Proposal which shows Canada has met its burden. As a result, the Proposal unconstitutionally trespasses on civil liberties in its current form.

#### Module 2: Modifying the Legal Framework

Module 2 proposes revisions to the *Canadian Security Intelligence Act* ("*CSIA*") which are contrary to Supreme Court of Canada jurisprudence on this subject. This is the only place in the Technical Paper where the Government has acknowledged that it is seeking feedback, despite the invitation on the Have Your Say page to "submit comments" on the Proposal more generally.

We are opposed to the "simplified process" vaguely proposed in this section of the Technical Paper for CSIS to obtain basic subscriber information ("**BSI**"). We are aware of no reason why CSIS should be authorized to bypass well established laws on search warrants, which protect individual rights and freedoms against unreasonable search and seizures. With respect to hate speech, the expediency sought by this section would in almost all circumstances be unnecessary. It is not clear, seeing as this is a regulatory proposal, whether these amendments to the CSIA would be reserved for criminal behaviour or more generalized investigatory procedures.

<sup>&</sup>lt;sup>26</sup> R v Carter, at para 94, citing R v Oakes, [1986] 1 SCR 103.

Further, it is unclear what the Discussion Guide considers to be an "online threat actor". To anchor such an impressive power of rushed warrants with a government intelligence service, based on an ambiguous and fear-mongering term, is problematic and irreconcilable to our democratic institutions, *Charter* values, and common law.

#### Privacy Issues

The Proposal seems designed to bypass the Supreme Court of Canada's decision in *R v Spencer*, 2014 SCC 43. In *Spencer*, the Court considered when BSI could be obtained. As noted in the first line of that decision, "the internet raises a host of new and challenging issues about privacy." It appears that the Proposal has not given sufficient consideration to issues about privacy. Obtaining BSI is a search, and such searches should be conducted with judicial authorization and otherwise meet the requirements in the case law and should respect *Charter* protected rights under section 8. There is insufficient detail in the Proposal to believe that those rights will be protected and respected in the expedited CSIS procedure contemplated. IPG expresses its disagreement with the proposed changes to the *CSIA*.

This same encroachment on section 8 rights is captured in the "Inspection Powers" section of the Technical Paper.<sup>27</sup> The pattern of *Charter*-infringing legislation shows that the Government has not paid due care to democratic values. As one commentator identified, these powers seem to create a "new internet speech czar" and "speech police",<sup>28</sup> powers that are usually associated to autocratic governments, not ones who should be guided by constitutional values and human rights.

#### 3. Conclusion

In summary, the Proposal:

i. has a problematic foundation in Bill C-36;

<sup>27</sup> Technical Paper, paras 88-93.

<sup>&</sup>lt;sup>28</sup> Corynne McSherry and Katitza Rodriguez, "O (No!) Canada: Fast Moving Proposal Creates Filtering, Blocking and Reporting Rules - and Speech Police to Enforce Them" (2021 August 10) Electronic Frontier Foundation, available online at: https://www.eff.org/deeplinks/2021/08/o-nocanada-fast-moving-proposal-creates-filtering-blocking-and-reporting-rules-1

- unreasonably and undemocratically infringes on rights guaranteed by section 2(b) of the *Charter* by constraining what can be said or seen on OCSPs (and other internet sites later prescribed by the Governor in Council);
- iii. puts unreasonable obligations on OCSPs which will invariably result in risk averse responses that unreasonably stifle free expression;
- iv. fails to reflect recent jurisprudence from the Supreme Court of Canada on privacy and subscriber information;
- creates unreasonable obligations and gives improper authority to OCSPs to determine whether they have "reasonable grounds to suspect" that the harmful content may reflect imminent risks to people or property and then report that suspicion to law enforcement, presumably for criminal investigation (despite the assertion that this is supposedly a regulatory proposal);
- vi. fails to respect current jurisprudence on section 8 Charter rights; and
- vii. creates ample opportunity for bias, discrimination, and inequal application of the law by creating an arbitrary and unworkable system.

We note that there is extensive commentary online by experts in this space that also raise serious issues with the Proposal. We have done our best not to duplicate their comments, but adopt and agree with the critiques put forward by Michael Geist in "Picking Up Where Bill C-10 Left Off: The Canadian Government's Non-Consultation on Online Harms Legislation" and Daphne Keller in "Five Big Problems with Canada's Proposed Regulatory Framework for "Harmful Online Content"". We also suggest that you review the "26 Recommendations on Content Governance: A guide for lawmakers, regulators and company policy makers" issued by AccessNow, which provides extensive guidance on the regulation of internet content which reflects democratic principles and respects human rights, something which the current Proposal fails to do.

The IPG opposes the Proposal and expresses a serious concern to the harmful effects on freedom of expression and principles of law that will ensue if the Government moves forward with the Proposal. We expect that the Government

Dissument common and an arresten la Lao ana familio a Tortarmalian Document indescent ana anna to the Access is interministe art

will take our criticisms into account and will cease its pursuit of the Proposal in its current form.

Yours truly,

Cal Mer

Candice Malcolm
Independent Press Gallery



CANADIAN CENTRE for CHILD PROTECTION

CENTRE CANADIEN de PROTECTION DE L'ENFANCE

September 24, 2021

Digital Citizen Initiative, Department of Canadian Heritage 25 Eddy Street GATINEAU, Quebec K1A 0S5

#### Re: The Government's proposed approach to address harmful content online

Thank you for giving the Canadian Centre for Child Protection ("C3P") the opportunity to provide comments on the discussion guide and technical paper released by the Government of Canada in respect of the Government's proposed approach to address harmful content online.

# About the Canadian Centre for Child Protection

C3P is a registered Canadian charity dedicated to the personal safety of all children. Our focus is on providing programs and services aimed at reducing child sexual abuse ("CSA") and the online sexual victimization of children. Since 2002, C3P has been operating Cybertip.ca, Canada's national tipline for the public reporting of online child sexual exploitation. In May, 2004, Cybertip.ca was adopted under the Government of Canada's *National Strategy for the Protection of Children from Sexual Exploitation on the Internet.* Cybertip. Receives and processes tips from the public about online crimes against children and refer any potentially actionable reports to the appropriate police unit and/or child protection agency. Our trained analysts assess and categorize child sexual abuse material in the course of processing reports as well as to support image takedown initiatives such as Project Arachnid (described below).

C3P also created and operates Project Arachnid, an innovative tool which helps combat the growing proliferation of child sexual abuse material ("CSAM") on the internet by detecting where known CSAM is being made publicly available and issuing notices to the entity hosting the material to request its removal.<sup>1</sup> Processing tens of thousands of images per second, Project Arachnid detect content at a pace that far exceeds that of traditional methods of identifying and addressing this harmful material. As of September 1, 2021, over 8.5 million notices have been sent to providers requesting content removal via Project Arachnid.

Our work has enabled us to gather data that highlights weaknesses in the current self-regulatory model that has been permitted in respect of online communication services. The real-world insight derived from this data puts our organization in a unique position to provide concrete feedback with a goal of achieving a regulatory response that will have the best possible outcomes for children. C3P is well positioned to be part of the solution in addressing the online sexual abuse and exploitation of children through flagging and issuing of removal notices associated with CSAM and harmful and abusive<sup>2</sup> images/videos of children.

<sup>&</sup>lt;sup>1</sup> Approximately 85% of the notices issued to date relate to victims who are not known to have been identified by police. See more at <a href="https://projectarachnid.ca/en/">https://projectarachnid.ca/en/</a>.

<sup>&</sup>lt;sup>2</sup> Harmful and abusive imagery/videos refers to material that does not meet criminal definitions but further victimizes the child because it is directly or indirectly associated with the abuse.

| CENTRE CANADIEN de CHILD PROTECTION PROTECTION DE L'ENFANCE

# Summary of position

C3P is strongly in favour of the federal government making social media platforms and other online communication services more accountable and transparent when it comes to combating harmful content online. We are especially pleased to see that the proposal contemplates:

- a broader definition of child sexual exploitation content than that which is articulated in the Criminal Code:
- provisions to facilitate access to basic subscriber information and transmission data when reports are made to police under the Mandatory Reporting Act, as well as the extension of time for which a provider must retain records associated with a report;
- an expansion of what gualifies as non-consensual distribution of intimate images, to that "for which is it not possible to assess if a consent to the distribution was given by the person depicted in the image or video"; and
- a requirement that accessible and easy-to-use flagging mechanisms for harmful content be instituted by OCSPs, and that clear content moderation guidelines be published by those subject to the regulatory regime.

We have several questions and concerns related to the model that has been proposed, and with our role as it relates to both child sexual exploitation content and intimate images. Particularly in relation to child sexual exploitation content, we urge the government to carefully consider all the progress that has been made in tackling this issue as a direct result of Project Arachnid, and our Cybertip.ca program. Our agency has a significant amount of experience dealing directly with industry on content removal, as well as victims who are desperate to have the content removed from public view. We know, all too well, that delays in removal can be devastating for victims, and can cause irreparable damage. Every minute that content remains available compounds the harm and increases the safety risk for victims, which risks include harassment and stalking in person and online.

We also know that there is often more than one company involved in making content available and therefore able to act to supress it from public view. It has been our experience that while there are bad actors out there at the host level, most upstream providers have little tolerance for hosting this type of material and are prepared to enforce their own contracts against the host once they become knowing of the nature of the material. In that regard, we refer you to our report issued in June, 2021 titled Project Arachnid: Online Availability of Child Sexual Abuse Material. An analysis of CSAM and harmful-abusive content linked to certain electronic service providers (the "Project Arachnid Report"), particularly the diagram on page 27 and the narrative on page 28 which sets out the different players in the internet ecosystem. As the report highlights, all of these players play a role in making content available to an end user and must be considered in the regulatory schema. We urge the government to consider all of the recommendations made within the Project Arachnid Report as it moves forward with its plans.

A strong concern that we have on the child sexual exploitation side is that if the process becomes overly prescriptive and bureaucratic at the outset, it may reverse the gains that have been made thus far on the voluntary side of the equation. Time is of the essence dealing with child sexual exploitation content and there needs to be a fast track to removal. This is something that could be facilitated by an organization



like ours, which has the skills and the expertise to focus in and target CSAM, harmful/abusive material to children and the non-consensual distribution of intimate images.

We understand that these are complex matters, and that there are still many issues to resolve before moving forward with any legislation. However, from our perspective, it is essential to keep the privacy, dignity and best interests of children at the forefront of any content removal strategy. While we recognize that other groups are vulnerable, as a society we owe unique duties of protection to children which are enshrined in international treaties such as the *Convention on the Rights of the Child*, *1989*, C.T.S. 1992/3; 28 I.L.M. 1456; 3 U.N.T.S. 1577; G.A. Res. 44/25 (ratified by the Canadian government on December 13 1991) (the "UNCRC"), and the Optional Protocols to the UNCRC.<sup>3</sup>

Below we have set out a general summary of our questions and concerns, using the general headings that are included in the Discussion Guide and Technical Paper published in the summer of 2021 by the Government of Canada. Following that are additional concerns and issues we would like to raise regarding the proposed model. We welcome the opportunity to engage constructively with the Government of Canada as it moves forward, and applaud the efforts of this government to work towards solutions for online harms.

## Module 1(A)

#### Handling jurisdictional issues and enforcement

The Technical Paper defines an Online Communications Service ("OCS") as "a service that is accessible to persons in Canada, the primary purpose of which is to enable users of the service to communicate with other users of the service, over the Internet". We would like to better understand the information the government proposes to authorize the Digital Safety Commissioner to collect from an Online Communications Service Provider (OSCP) to determine if the Act should apply to such OSCP. We believe we have gained significant insight into the various ways in which internet companies structure their operations and will be able to assist in identifying the type of information that is likely to be helpful to the determination that must be made.

In addition, we are interested in better understanding how the government envisions that the Act will be applied and enforced with respect to companies that seemingly have no physical footprint (e.g. servers, offices, staff) in Canada, such as Parler, Gab, Reddit, Tik Tok, etc.

# Module 1(B): New rules and obligations

#### Addressing child sexual exploitation content

The Technical Paper states in Module 1(A) that:

<sup>&</sup>lt;sup>3</sup> The Optional Protocols to the UNCRC are the *Optional Protocol to the Convention on the Rights of the Child on the Involvement* of children in armed conflict, the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child* prostitution and child pornography, and the *Optional Protocol to the Convention on the Rights of the Child on a communications* procedure. Also relevant is General Comment 25 and other documents published to aid in interpretation and implementation of these obligations. More information can be found here: <u>https://www.ohchr.org/EN/HRBodies/CRC/Pages/CRCIndex.aspx</u>

CANADIAN CENTRE far CHILD PROTECTION

The concept of child sexual exploitation content should capture 1) criminal law offences in this area set out in the <u>Criminal Code</u>, in a manner adapted to a regulatory context, including child pornography and other sexual offences relating to children; and 2) material relating to child sexual exploitation activities that may not constitute a criminal offence, but when posted on an OCS is still harmful to children and victims (e.g., screen shots of videos that do not include the criminal activity but refer to it obliquely; up-to-date photos of adults who were exploited/ abused as children being posted in the context of their exploitation and abuse as children).

As stated in our summary position, we are very grateful to see child sexual exploitation content being defined more broadly than what is criminal. This is similar to the way in which we approach the issue of removal as an organization. For more information about how we approach these matters, please see our report titled <u>How we are failing children: Changing the paradiam (the "Framework"</u>). We urge the Government to consider going even broader than is currently contemplated and include material that depicts violence or sadistic acts against children as is set out in the Framework. Not all content that is harmful to children is sexual in nature, and our organization has been made aware in the past of videos depicting violence against children. Such depictions are clearly harmful, but in Canada, the recording and sharing of such depictions is still not illegal, so not all providers will act to remove such content when it is brought to their attention.<sup>4</sup>

However, we noticed that in Module 1B, the obligation of an OCSP to address harmful content that will be covered by the Act is really occurring in two discrete steps. First, the obligation is to respond to the person complaining as to whether the definition of harmful content is met or not, and if it is met, the obligation is to then "make that harmful content inaccessible to persons in Canada".

Our question about the "inaccessible" component of this is set out below, but first we would like to flag that under this model, if the OSCP responds that the content does <u>not</u> meet the definition, it will then have met its obligations. This means it will be up to the user who reported the content to compel a review of the decision, which may or may not resolve the matter thus requiring further escalation. We also note that both the poster of the content and the complainant have a right of appeal, and that there is recourse the Digital Recourse Council of Canada only <u>after</u> all avenues have been exhausted at the OCSP level. This puts a tremendous burden on complainants, and assumes that all complainants will be motivated to push an issue through to that level.

Moreover, while all of this is going on, it appears the alleged child sexual exploitation content would remain available and in public view. In addition, this model envisions several people along the chain who will be looking at the child sexual exploitation content. In our view, all of this needs to be thought through in more depth, and through a trauma-informed lens. As an example, if content is reported as child sexual exploitation material, we believe that unless it is patently plain and obvious at the initial review that the content is **not** of a child at all (e.g., it is a picture of a bird, or it is unequivocally an adult person), the

<sup>&</sup>lt;sup>4</sup> Violent content involving children has been tackled in other countries however. For example, in 2017, Australia amended section 51A of its *Crimes Act* (akin to Canada's *Criminal Code)* to replace the term "child pornography" with the term "child abuse material". The definition for this new term was expanded to encompass material that depicts "torture, cruelty or physical abuse (whether or not the torture, cruelty or abuse is sexual)"



material should be promptly made inaccessible to allow the review process to play out. This will help to decrease the harm and extensive revictimization to the child that could ensue should the initial assessment have been inaccurate, particularly considering how rapidly content can propagate when left to fester online.

#### Removing content vs. making it inaccessible in Canada

In terms of making the content inaccessible, is it accurate to say that a company would not be expected to remove content globally (as opposed to geo-blocking in Canada) in the following two cases?

- CSAM-adjacent material that may not be illegal (i.e., the second type of child sexual exploitation content defined in Module 1(A);
- Material that is illegal in Canada (e.g., a written child pornography story) but may not be illegal in other countries?

In terms of material that is categorically illegal (e.g., at a bare minimum, material that meets the Interpol baseline criteria<sup>5</sup> as being illegal CSAM in most countries of the world), more must be done than simply making it "inaccessible". For example, we would also like to suggest that the images/hash values for child sexual exploitation content that is made in accessible/subject to blocking be made available not only among OCSPs (to prevent the same material reappearing on another OCSPs service), but also to our organization so they may be injected into Project Arachnid. In addition, we suggest that any order that may be made in relation to child sexual exploitation content be permanent, as opposed to expiring after a period of time. This is because of the illegal nature of the content.

Further, we suggest it be required that content, once made inaccessible or subject to blocking (or ordered to be made inaccessible or blocked), must not reappear on the same service. The reason we suggest this is because we know that the issue of image recidivism (meaning an image flagged or assessed as problematic reappearing on the same service) is a persistent problem. For more information on this, please see the report we issued in June, 2021 titled <u>Project Arachnid: Online Availability of Child Sexual</u> <u>Abuse Material. An analysis of CSAM and harmful-abusive content linked to certain electronic service</u> <u>providers.</u>

Related to the above, we wish to flag that blocking content will be ineffective in relation to individuals who have even minimal technical abilities within Canada, and will absolutely not be effective in relation to anyone outside of Canada, which means the victimization of the child will continue globally. It also may promote a false sense of security for the victim, who may not understand that the blocking is geographical only, and that their images are still accessible and available worldwide. The widespread availability and accessibility of VPNs, the Tor network, etc. cannot be ignored and accordingly we urge the government to reconsider this approach particularly in relation to child sexual exploitation material.

<sup>&</sup>lt;sup>5</sup> INTERPOL. (2018). Towards a global indicator on unidentified victims in child sexual exploitation material: Technical report. https://www.ecpat.org/wp-content/uploads/2018/02/Technical-Report-TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-

MATERIAL.pdf states that baseline images must: depict a real, prepubescent child (no sign or very first signs of puberty, under 12 or 13), who is involved in or witnessing sexual/abuse activities; and the media must have a clear focus on the child's sexual/anal area. This definition is exceedingly more restrictive than the scope of what is actually illegal in most countries.



CENTRE CANADIEN de PROTECTION DE L'ENFANCE

#### Country of residency of complainant or aggrieved person

Will a non-Canadian resident be able to access the prescribed regulatory process to have content removed or made inaccessible in Canada?

# Module 1(C): Establishment of the new regulators

#### Conflicts of interest

We note that the person appointed as Commissioner or Deputy Commissioner, and well as members on the Digital Recourse Council and the Advisory Board, must not be a *shareholder* of an OCSP. We believe this limitation is insufficient to ensure there is no conflict of interest, and that decisions are not polluted by considerations that are not squarely focused on child protection. We are also puzzled as to why an OCSP has a place at the table at all, particularly in relation to child sexual exploitation matters. In our view, given the integral role that the Commissioner and Deputy Commissioner will play in this space, it is essential that they have no ties to an OCSP of any kind. As such, we recommend that any person who is employed by an OCSP, or who derives income or profit from an OCSP, should also be excluded from the role of Commissioner and Deputy Commissioner, as well as from having a place on the Digital Recourse Council or the Advisory Board.

#### Advisory Board Composition and Appointment

We note that the proposed Advisory Board will be made up of subject matter experts from various disciplines, including OCSPs. It also appears that the Advisory Board will be the same for all five types of content at issue. In our view, there ought to be a specialized Advisory Board for the purpose of child sexual exploitation content matters that is comprised of members with expertise related to children generally, and exploited children specifically. This particular Advisory Board should also be required to make decisions in the best interests of children, consistent with Canada's obligations under the *Convention on the Rights of the Child* and its related documents.

Moreover, given our organization's experience in dealing with child sexual exploitation material for the last 20 years, we believe it is appropriate that our organization be represented on the Advisory Board.

We are also concerned that the Advisory Board appointees are appointed by the Minister "at pleasure" and would like there to be more discussion around the reasons for this. In our view, making the appointment at the pleasure of the Minister makes it seem like more of a political appointment and raises a risk of the appearance of political interference in the advisory board process.

#### **Right of Appeal**

We note that there is a contemplated right of appeal to the Personal Information and Data Protection Tribunal. We suggest that given the sensitivity and potential illegality of child sexual exploitation materials a court of competent jurisdiction may be a better choice. If the government proceeds with a Tribunal model, there will likely need to be additional precautions and safeguards in place for such appeals, similar to the way in which the courts handle illegal and sensitive materials.



| CENTRE CANADIEN de CHILD PROTECTION PROTECTION DE L'ENFANCE

#### Monitoring compliance

The Technical Paper contemplates that the Digital Safety Commissioner will monitor OCSP compliance with an inaccessibility order. We would like to better understand how this may be done. From our experience, automation of this aspect will be required as a manual monitoring process will be completely unfeasible and ineffective.

#### In camera meetings

We note that the Digital Safety Commissioner and the Digital Recourse Council of Canada may conduct hearings in camera for a variety of reasons. We completely understand that there may be a need for in camera proceedings, however, have grave concerns about the inclusion of "confidential commercial interests" in the list of reasons for which an in camera proceeding may occur. In our view, the matters to be considered by these bodies are in the public interest and accordingly the scope of in camera proceedings should be narrow and carefully circumscribed to mirror the open court principle which guides court proceedings.

# Module 1(D): Regulatory powers and enforcement

#### Naming an OCS and OSCP publicly

Paragraph 83 of the Technical Paper contemplates that the Digital Safety Commissioner and the Digital Recourse Council of Canada have discretion over whether to name the OCS and OCSP publicly, as well as the timing of the publication. We are concerned that this discretion will greatly reduce the effectiveness of the regulatory regime as whole, and note that the Privacy Commissioner of Canada also did not name entities for several years. Rather than blanket discretion, consideration should be given to setting out criteria, with the default being to name the companies except in narrow, prescribed circumstances.

#### Factors in determining Administrative Monetary Penalty

In addition to the factors set out in paragraph 98 and 107 of the Technical Paper, we would note that in the area of child sexual exploitation, consideration should be given to including consideration of aggravating and mitigating factors that would be applicable in a criminal law context. As an illustrative example, we suggest having a look at the case of R v YesUp ECommerce Solutions Inc., 2020 CarswellOnt 19731 (ONCJ), which is the only known case in Canada in which a company was prosecuted for a child pornography offence. More background on this prosecution can be found in R v YesUp ECommerce Solutions Inc., 2013 ONSC 6884 (CanLII), <http://canlii.ca/t/g1rm6>. Note that individual employees of the company were also prosecuted for failure to report under the Mandatory Reporting Act. Those cases are reported at: R v Kok, 2020 CarswellOnt 19729 (ONCJ) and R v Li, 2020 CarswellOnt 19730 (ONCJ).

# Module 2: Modifying Canada's existing legal framework

#### Clarity on C3P's continuing role under the Mandatory Reporting Act

The Discussion Guide recommends that the proposed legislation should amend An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service ("Mandatory Reporting Act") to:



Centralize mandatory reporting of online child pornography offences through the <u>Rayal</u> Canadian Mounted Police's <u>National Child Exploitation Crime Centre (NCECC)</u>;

However, under a regulation made pursuant to section 2 of the Mandatory Reporting Act, C3P is currently the designated agency (in regulations) to receive URLs that may contain child pornography and are required to be reported under section 2.

The Technical Paper is more precise, in that it proposes that the NCECC be the designated agency "for reports made under section 3" of the Mandatory Reporting Act. However, as the Discussion Guide states the proposed change much more broadly, we would appreciate the government confirming to us that C3P will remain the designated entity to receive reports under section 2 of the Mandatory Reporting Act. There were significant policy considerations that went into naming our organization as the designated entity under section 2 which we would be happy to discuss further with your office.

#### Defining which service providers are subject to mandatory reporting

In addition, the Technical Paper states that:

"The Act should amend the <u>Mandatory Reporting Act</u> to ensure that it applies broadly to all types of Internet services and that definitions are sufficiently flexible and non-exhaustive to encompass rapidly evolving technological developments."

In our view, this is a key component for a successful mandatory reporting regime. Our question is how will the various service providers be notified of their obligations? One shortcoming of the Mandatory Reporting Act when it was originally introduced is that there was no formalized communication plan that occurred and thus it largely fell to our organization and police to explain to companies what their obligations were.

A related question is how non-compliance of the Mandatory Reporting Act will be monitored and enforced. It appears that annual reports will be made by the NCECC but it is unclear what will occur beyond that.

#### Satisfying reporting obligations

We have some concerns about the exception that permits companies to meet their obligations under the Mandatory Reporting Act by reporting to an entity in another jurisdiction. While we do understand the efficiencies from the perspective of an OCSP, this does mean that Canadian reports are processed in a foreign country first and assumes that there will be no delays or other issues that will result from that. We would like to propose that it be required that all such reports should be required to be copied to police and/or our agency (as appropriate) to ensure that the necessary information to address the matter is received in Canada at the earliest possible opportunity.

# Other Considerations

The foregoing are specific considerations and concerns related to the specifics of the proposal. The following are additional considerations that do not necessarily relate to one discrete aspect of the proposal:



| CENTRE CANADIEN de CHILD PROTECTION PROTECTION DE L'ENFANCE

#### Knowledge of context of images

More discussion and planning will be needed to determine how an OCSP, and the Digital Resource Council, will be able to know that a non-CSAM image is connected to known child sexual abuse survivors. Our organization has significant expertise in this regard which could be leveraged by the Government of Canada as it implements this initiative.

#### Content/image recidivism

As discussed above, it has been our experience that previously flagged images will often reappear on a platform that has previously removed the same image. This is especially the case when the image is of an adolescent/pubescent victim. Given today's technology, there is no need for this to occur and in our view the proposed regulation must enact clear and consistent rules to ensure that child sexual exploitation images are not reappearing on platforms. This will help avoid situations where content must be flagged repeatedly, and it will also reduce duplication by ensuring that once an image is flagged for removal, it does not reappear.

#### Disrupting the ongoing sharing of CSAM and harmful/abusive material

When content is deemed illegal or harmful to children by the Digital Recourse Council, we suggest that the images or hash value should be shared with C3P for the purpose of ingesting into Project Arachnid. Project Arachnid is an established tool for identifying known images of CSAM and harmful/abusive material which automates the issuance of removal notices to providers. It is survivor-centric and its purpose is to disrupt the ongoing sharing of this material at global scale, which is far broader than blocking Canadians from viewing the material. Survivors have told us clearly that the ongoing dissemination of their abuse material is a continuing source of harm and from their perspective, quickly disrupting and stemming that distribution is one of their top concerns. To gain a greater understanding of the views of survivors, please see our Survivors' Survey, the results of which were published in 2017 and which is posted at the following URL: https://www.protectchildren.ca/en/resources-research/survivorssurvey-results/.

#### Funding Model

We note that it is contemplated that the operating budgets for the Digital Safety Commissioner and Digital Recourse Counsel will be funded by the regulated entities. We appreciate that this may be a common funding model for regulating entities, however we strongly urge the government to reconsider the optics of directly linking the funding of these offices to the very entities being regulated by it. In our view, there is an inherent conflict of interest that is likely to develop should this type of regulator set up with this type of funding model.

# Conclusion

In summary, we appreciate the opportunity to submit our feedback to the proposal, and are very interested in having the opportunity to engage in meaningful dialogue with the Government of Canada as it moves ahead with this important initiative.

Sochards and Sochard and Social and Socia

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St Gatineau QC K1A 0S5 Email: <u>pch.icn-dci.pch@canada.ca</u>

September 25, 2021

Dear Digital Citizen Initiative,

This submission responds to the Government of Canada's invitation for feedback on its proposal for a new legislative and regulatory framework for addressing online harms. As Canadian academic researchers who specialize in either legal or technical aspects of privacy and security, we are concerned about the proposals to require the mandatory reporting of basic subscriber information (BSI) and transmission data without judicial authorization.

In our view, both BSI and transmission data attract a reasonable expectation of privacy and so engage s. 8 of the *Charter*. We remain skeptical that either type of this information can be conveyed to police without a warrant or court order, which is the traditional legal protection against the exercise of overbroad police discretion to intrude upon privacy. However, for the sake of fleshing out additional issues we have written this submission assuming that there are some circumstances where mandatory reporting of BSI or transmission data may be justified and not open to the kinds of abuse that judicial authorization is meant to prevent. We therefore begin by accepting that circumstances where a child pornography offence is "clearly evident" may be one of those rare circumstances, if that threshold is properly crafted. However, a law requiring the reporting of such information without prior judicial authorization is only "reasonable", and therefore constitutionally permissible, if this reporting is limited to very specific purposes, there are technical safeguards to minimize privacy risks and potential misuse, and there is some form of independent oversight. The Government of Canada's proposals fall short on all of these fronts. We elaborate on each of these points below.<sup>1</sup>

#### Reasonable Expectation of Privacy

BSI is not formally defined in the Discussion Guide, but is stated to include "customer's name, address, phone number, billing information associated with the IP address". In *R v Spencer*, the Supreme Court of Canada held that BSI attracts a reasonable expectation of privacy and that police access therefore requires a warrant unless a reasonable law authorizes it.<sup>2</sup> The Supreme Court rejected the approach that looked at the information in isolation (as "simply a name,

<sup>&</sup>lt;sup>1</sup> See also Lisa M Austin and Andrea Slane, "Digitally Rethinking Hunter v. Southam" (May 3, 2021), available at SSRN.

<sup>&</sup>lt;sup>2</sup> R v Spencer, 2014 SCC 43.

address and telephone number matching a publicly available IP address"<sup>3</sup>) and held that in contexts where there is controversy regarding defining the subject matter of the search,

the Court has taken a broad and functional approach to the question, examining the connection between the police investigative technique and the privacy interest at stake. The Court has looked at not only the nature of the precise information sought, but also at the nature of the information that it reveals.<sup>4</sup>

In other words, the Supreme Court held that we need to look at the use-context of the information in order to understand whether it attracts a reasonable expectation of privacy. In the context of the proposed new regime, BSI would be required in "cases where a child pornography offence is clearly evident" and therefore would link a particular person to such cases. This sounds very much like the use-context of *R v Spencer*, where the Supreme Court required a warrant. Therefore the use of BSI in the online harms context attracts a reasonable expectation of privacy.

"Transmission data", as used in the Discussion Guide, follows the *Criminal Code* definition (s. 487.011) and means data that:

(a) relates to the telecommunication functions of dialling, routing, addressing or signalling;

(b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2), in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and

(c) does not reveal the substance, meaning or purpose of the communication.

Transmission data so defined can be used in ways that are highly privacy-invasive. For example, the boundary between the data listed in ss.(b) and (c) is highly unstable. Information about source/destination IP addresses and port numbers can be used to infer the type of traffic, and information about size can be used to infer content. Techniques like traffic fingerprinting are surprisingly accurate, and the timing and sizes can give you information as granular as *which* youtube video someone is watching.<sup>5</sup> Therefore the use of transmission data in the online harms context also attracts a reasonable expectation of privacy.

Warrantless access to either type of information could still be constitutionally permissible if authorized by a reasonable law. In our opinion, this requires limiting the purposes for which this

<sup>&</sup>lt;sup>3</sup> Ibid at para 24.

<sup>&</sup>lt;sup>4</sup> Ibid at para 26.

<sup>&</sup>lt;sup>5</sup> See, for example, Schuster et al., "Beauty and the Burst: Remote Identification of Encrypted Video Streams", USENIX Security 2017.

https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/schuster

information is used, implementing technical safeguards against misuse, and creating robust methods of independent oversight. We elaborate on this in the following sections.

#### Limiting Purposes: The "clearly evident" Threshold for Mandatory Reporting

There is a significant potential for violation of the right to be secure against unreasonable search and seizure if the conditions for triggering the mandatory reporting of transmission data and/or BSI are not clear. Currently, mandatory reporting requirements require an internet service provider to a) relay an IP address or URL to a designated organization where they have been advised that that location is one "where child pornography may be available to the public", or b) notify an authority where the service provider has "reasonable grounds to believe that their Internet service is being or has been used to commit a child pornography offence". The current requirements are both quite broad (in that they do not require service providers to verify whether child pornography offences are being committed through their services, leaving that to police) and quite limited (in the amount of information that is initially required to be conveyed to police). This is an acceptable balance between the need to inform police when a service provider becomes aware that a child exploitation crime is likely being committed through their services, and subscriber privacy. The expectation of the existing mandatory reporting requirement is that police will conduct further investigation, and will apply to a court for authorization to access transmission data or, following R v Spencer, BSI.

The Discussion Guide proposes a new and far more intrusive requirement for mandatory reporting. First, the proposal extends the mandatory reporting requirement to additional service providers (e.g. social media platforms). Second, it proposes an additional threshold for mandatory reporting in "cases where a child pornography offence is clearly evident", that would require including BSI or transmission data in the report. While this is a higher threshold than the existing circumstances that trigger mandatory reporting of less sensitive information (i.e. the IP address or URL), far more specificity and justification will need to be provided before we would be satisfied that an appropriate balance has been struck in this proposed regime.

With regard to the degree to which service providers will need to confirm that a child pornography offence has been committed, at present there is no indication in the materials provided as to how a service provider will determine that such an offence is "clearly evident". Service providers are not, and should not be, required to view child sexual abuse materials (CSAM) in order to establish that an offence is clearly evident. If this rule is maintained, as it must be, then that leaves only technological means that do not require a human to view materials in order to establish that such an offence is "clearly evident".

Are the guidelines only triggered where images have been identified as hash matches to images in a law enforcement CSAM database? If so, then we note that there are differences between the hash-matching programs used by different service providers, and that perceptual hash matches (which allow for close rather than only exact matches to be captured), while useful to capture images that have been only slightly altered to avoid exact match (cryptographic) systems, also stand a higher chance of false matches. We further note that Apple's recent announcements regarding its use of a perceptual hash matching system (NeuralHash) to report CSAM materials synced to upload to iCloud took account of this likelihood of false matches by setting a fairly high threshold of 30 matches from the same account before reporting to police. The current guidelines do not set such a threshold and seem to indicate that every match should be reported, along with the transmission data and/or BSI. As we outline below, the sensitivity of this data calls for greater protection against false positive matches. We suggest a higher match threshold is needed in the contemplated guidelines as well.

Further, if some form of automated searching for images by service providers is contemplated, then there must also be protections in place to address the possibility that such a system could be gamed. For example, it is technically feasible to create an image that would register as a match to an image in a CSAM database even though to the human eye the image is of something else. A malicious actor could in this way make an individual subject to a highly stigmatizing police investigation. A higher threshold of how many matches are required goes some distance toward guarding against such deliberate interference, and there should be new criminal offences for any such interference as well. However, in all cases there needs to be *independent verification* of whether the "clearly evident" threshold has been met before any transmission data or BSI is made available to law enforcement.

The verification process should not lie with the service providers: instead, if a hash match threshold is met, the RCMP's National Child Exploitation Crime Centre (NCECC) should determine if the matched files are indeed child pornography. Only once that has been verified should police be able to access transmission data and/or BSI (via technical safeguards outlined below), provided that the process is subject to independent oversight.

#### Limited Purposes and Technical Safeguards

The purpose outlined in the Discussion Guide for mandatory reporting of BSI is to expedite "police response". This is far too vague and ripe for abuse. If the issue is the difficulty in getting this information in a timely manner through the warrant process then the answer is not necessarily to get rid of the requirement for independent oversight to limit police discretion — which is a key function of the warrant requirement — but rather to redesign it.

The proposal in the Discussion Guide is to centralize mandatory reporting through the NCECC. Because of this centralization, the federal government also has the opportunity to put in place technical safeguards to ensure access controls, audit trails, and oversight by an independent body. This opportunity could be used to create an expedited process for access to BSI that does not sacrifice the constitutional requirement of prior (independent) authorization. For example, there could be mandatory reporting of BSI along with the evidence that an organization relied upon to determine "cases where a child pornography offence is clearly evident" but the BSI would be encrypted until there was independent verification of clear evidence of a child

4

pornography offence, whereupon it would be automatically decrypted. Unauthorized access to this information for other purposes would be mitigated through access controls and audit trails, with this audit available to the independent oversight body. We offer some further suggestions on oversight in the following section.

The Discussion Guide outlines that the purpose of providing transmission data is in order to allow the police to identify ISP and jurisdiction. However, this response is quite dramatically over-inclusive. All that is required to identify ISP and jurisdiction is the IP address. In fact, most of the data included in the definition of "transmission data" is not even useful for determining jurisdiction.

As we already outlined, the existing *Mandatory Reporting Act* already requires the reporting of an IP address where the service provider has been advised that this address may be making child pornography available to the public: it is not at all evident that this practice requires changing except to extend this requirement to a broader group of service providers. If the new "clearly evident" threshold contemplates other circumstances than where CSAM materials "may be available to the public", then these circumstances should be clearly identified in order to be included within the requirement to convey IP address. Asking for additional components of "transmission data" remains to be justified.

#### Oversight

Prior judicial authorization has long been held to be a core requirement when law enforcement seeks access to information that attracts a reasonable expectation of privacy.<sup>6</sup> In some cases, where the search is authorized by a reasonable law, and is narrowly tailored and accurate, courts have accepted after-the-fact review.<sup>7</sup>

As we outlined in the previous section, because the proposed mandatory reporting will be centralized through the NCECC, this provides an opportunity to create an independent oversight body that can provide independent authorization (whether prior to law enforcement use or, in some circumstances, as after-the-fact review) in a manner that can both meet the needs of law enforcement and still maintain constitutional safeguards.

The Discussion Guide proposes the creation of three new regulatory bodies (the Digital Safety Commissioner of Canada, the Digital Recourse Council of Canada, and an Advisory Board) but none of these bodies appear to fulfill the functions of independent oversight that we outline here. For example, the listed powers of the proposed Commissioner are very much focused on the content-moderation concerns of this proposal rather than oversight of law enforcement access to, and use of, BSI and transmission data. In addition to performing the function of oversight of the NCECC, such an independent body should have both significant technical expertise and community representation.

5

<sup>&</sup>lt;sup>6</sup> Hunter v Southam, [1984] 2 SCR 145.

<sup>7</sup> See, for example, R v Kang-Brown, 2008 SCC 18.

The Technical Paper accompanying the Discussion Guide indicates that the proposed legislation should make clear that "when using personal information obtained pursuant to the Mandatory Reporting Act, the police would be bound by the use limitation in federal legislation (the Privacy Act) for federal police and comparable provincial legislation for provincial and municipal police " (Module 2, para 6). The problem is that neither of these statutes provide an adequate statutory framework for preventing misuse. To give an example, the Privacy Act permits the use and disclosure of personal information "to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed".8 The regulations include CSIS, the Canada Border Services Agency, and many others as such specified investigative bodies. In other words, the Privacy Act would permit rather than constrain fairly broad sharing of BSI and transmission data, with no requirements that this be limited to specific offences or specific types of purposes. Similarly, provincial legislation like Ontario's FIPPA would permit the broad sharing of this information to another law enforcement agency in Canada or in a foreign country.9 These privacy statutes were never meant to be legislation to provide meaningful accountability in relation to law enforcement.

#### Conclusions

In conclusion, we think that the proposal for mandatory reporting of BSI and transmission data does not adequately protect Canadians' privacy;

- Both BSI and transmission data attract a reasonable expectation of privacy.
- The mandatory reporting proposal would broaden who has the obligation, their role in determining whether a child pornography offence is evident, and would require much more information to be reported than is currently the case.
- The proposal needs to provide clarification as to how service providers should determine when the reporting threshold has been met and provide additional safeguards against false positives and abuse of the system.
- The purposes for requiring BSI are vague and the purposes proposed for requiring transmission data do not justify access to anything other than IP address.
- The government should redesign, rather than jettison, independent oversight of police access to BSI and transmission data.
- The current proposals for new regulatory bodies and current privacy legislation do not provide adequate independent oversight.

<sup>&</sup>lt;sup>B</sup> See Privacy Act, RSC 1985, c P-21, ss. 7(b) and 8(2)(e).

<sup>&</sup>lt;sup>9</sup> See Freedom of Information and Protection of Privacy Act, RSO 1990, c F.31, ss. 41(1)(c) and 42(1)(f)(i) and (ii).

Seatharta - construction (Constant) (Constant)

Sincerely,

Lisa M. Austin Professor and Chair in Law and Technology Faculty of Law Associate Director, Schwartz Reisman Institute for Technology and Society University of Toronto

Glas

Andrea Slane Professor, Legal Studies Program Faculty of Social Science and Humanities Ontario Tech University

David Lie Professor and Canada Research Chair in Security and Reliable Computer Systems (Tier 1) Department of Electrical and Computer Engineering University of Toronto

10c

Ian Goldberg Professor and Canada Research Chair in Privacy Enhancing Technologies Cheriton School of Computer Science University of Waterloo

Decement communique, no initia de la Loi sur l'acoles à l'information ritocurrent resonnes que un mil. the accest is marmittent any.

# The Government's Proposed Approach to Address Harmful Content Online

# Submission to the Government of Canada

September 2021



2705, prom. Queensview Drive, Ottawa (Ontario) K2B 8K2 Tel. 613-820-2270 \\ Fax 613-820-7244 \\ Email acppu@caut.ca

www.caut.ca

Submission on Government's Proposed Approach to Address Harmful Content Online

September 2021

Founded in 1951, the Canadian Association of University Teachers (CAUT) is the national voice for academic staff representing 72,000 teachers, librarians, researchers, general staff, and other academic professionals at some 125 universities and colleges across the country. CAUT is an outspoken defender of academic freedom and works actively in the public interest to improve the quality and accessibility of post-secondary education in Canada.

As defenders of academic freedom, the right to teach, research, publish and express opinions without fear of political or institutional censorship, CAUT has grave concerns about the online harms bill the government intends to introduce in the autumn of 2021.

At this time, CAUT urges the government to reconsider this legislative project. The proposed approach described in the consultation's technical paper and discussion guide is rife with unintended, serious, and harmful consequences. The kind of regime being considered by the government would inadvertently censor legal speech and undermine the rights and civil liberties of Canadians.

# Proposed approach

The proposed framework requires content platforms— Online Communication Service Providers (OCSP)—to police and remove content that falls into one of the five categories of "online harms." This includes the use of machine learning and Artificial Intelligence (AI) to proactively search for harmful content. Users could also indiscriminately flag any content as potentially being illegal. Once content is flagged, OCSPs will have 24 hours to remove it. OCSPs will also have to report content they remove directly to the RCMP, CSIS or both without notifying the user.

A new 'Digital Safety Commissioner' would be created to oversee this regime, though they would not report to Parliament. This is problematic because, among other things, the Commissioner would have the power to conduct hearings on content takedowns in secret, justified by privacy, commercial and industrial secrecy, national security and defense, and international relationships with other governments. The harmful content targeted by this legislation is wide-ranging and poorly defined. It includes terrorist content; content that incites violence; hate speech; non-consensual sharing of intimate images; and child sexual exploitation content. CAUT acknowledges the deep harm this content can cause, especially to vulnerable individuals and marginalized groups. We do question whether the proposed approach is indeed the best tool at this time to address the problems of these online harms given that they are already offences in Canada's *Criminal Code*. CAUT is also doubtful whether the introduction of one single regulatory regime is the best way to address the variety of online harms targeted by this legislation.

# Systemically flawed

The imposition on OCSPs to determine what is lawful content is problematic. The proposed approach is systemically flawed to incentivize OCSPs to be overvigilant and over-remove content. Some ways the government has designed this system to encourage hyper-vigilance on the part of OCSPs include:

- The speed with which OCSPs would be required to remove flagged content (24 hours);
- The sheer volume of content that would have to be moderated; and,
- Stiff penalties which the Digital Safety Commissioner would be empowered to impose (whichever is greater of either 3% of a OCSP's global revenues or \$10 million dollars.)

Further indications that the government's proposal is systemically tilted towards censorship includes the proposal for a 'Digital Recourse Council'. This body of 3-5 people would hear appeals from users regarding OCSP's moderation decisions. The Council's decisions, curiously, would be binding in the instance of OCSP content takedowns but non-binding for the re-instatement of content.

Another dimension for consideration in the proposed approach is the potential for it to be used by malicious internet actors as a tool to silence and abuse innocent individuals and communities, particularly those who are already marginalized. Giving users the opportunity to report on others can be weaponized, especially by Submission on Government's Proposed Approach to Address Harmful Content Online

September 2021

organized groups of internet vigilantes or crusaders operating to advance a particular viewpoint or political agenda. Though user reporting is already a mainstay of OSCP moderation today, responsible OSCPs cannot necessarily do their due diligence in responding to these reports if the government imposes upon them the added pressure of speed and financial penalties. The result is that OSCPs will be incentivized to remove content and lock accounts of innocent parties under attack from internet trolls.

# Distinguishing between legal & illegal content

Distinguishing between legal speech and illegal content is not always simple and obvious. In our democratic society, much that is awful, is likely also lawful speech, as the courts have set a high bar for what constitutes prohibited hate speech. Nonetheless, the ability to distinguish between lawful and illegal is difficult; even the courts struggle to do this with legal experts, rigorous arguments, and an ample amount of time for open and transparent inquiry.

The difficulties of making this distinction between illegal content and legal speech are only exacerbated when the task is given to machine learning and AI, which cannot necessarily understand the entire context in which content exists and operates.

- Examples of how legal content might be misidentified and removed by OSCPs if algorithms fail to fully grasp the context of content and statements.
- Academic researchers investigating unpopular or controversial topics may use OSCPs to exchange and share information. This new legislation and onus on OSCPs to police and remove content could have an impact on academic research and extra-mural speech.
- Protest literature, sociopolitical satire, conflict photography<sup>1</sup>, or the documentation of human rights abuses could undermine civil disobedience

 The iconic Pulitzer Prize winning photo of the naked Vietnamese nine-year-old girl running away from a napalm attack was misidentified by Facebook as child pornography and taken down in 2016. It took an international backlash for the platform to reverse and censor voices looking to bring important nuance and debate to sensitive subject matters.

- Artists, museums, galleries, and art educators use image content, like nude art, to promote exhibits, public lectures, and other research that could be misidentified as sexual content.<sup>2</sup> Quick content takedowns and the lengthy complaint and recourse regime could have a significant impact on the ability to promote events that are substantial revenue generators for those working in the cultural sector.
- Vulnerable individuals and marginalized groups frequently come together in online spaces to find community, seek out support and discuss their experiences. If these discussions include relaying information about experiences of discrimination or attacks, AI surveillance could wrongfully flag this content as online harm.

In the last example, censoring this legal speech would have the unintended consequence of exacerbating the existing, well-documented pattern of online speech policing and removal targeting equity-deserving individuals and communities. Further to this point, relying on machine learning and AI could perpetuate social inequities given issues around algorithmic biases and insufficient access to the full breadth of training data used by OCSPs.

# Privacy concerns & unwarranted surveillance

Moderating and decontextualizing online content is further complicated when considering that OCSPs, under the proposed approach, are required to report to security agencies when content is flagged harmful, opening the door to unwarranted surveillance of academics and researchers. Whether through human or AI-generated moderation, under this scheme the government is incentivising private companies to moderate, make determinations of, and share data and

its decision. See, BBC News "Fury over Facebook 'Napalm girl' censorship" (09 September 2016).

3

Hyperallergic "Facebook Censors Art Historian for Posting Nude Art. Then Boots Him from Platform" (27 November 2018).

Seathanta - construction to scale) in 1997 - Dia Sy Construction Supervised Construction of the 1998 - Construction of the

Submission on Government's Proposed Approach to Address Harmful Content Online

information on suspected criminal activity, without alerting affected individuals.

The proposed legislative and regulatory framework would only further institutionalize and grant security agencies with powers to collect data and monitor information about Canadians, with no commensurate increase in oversight or accountability. Academics and researchers could be subjected to surveillance creating a chill on political discourse that challenge dominant paradigms. The technical paper provides little clarity on limitations to interagency information sharing or time limits for how long security agencies are permitted to collect and store data and information.

### Summary

CAUT supports net neutrality, the principle that Internet Service Providers should enable access to all content and applications regardless of the source, and without favoring or blocking particular products or websites. The development of an open Internet has been instrumental in dramatically expanding both research capability and learning opportunities for Canadian academics, researchers, and students. The government's proposed approach to addressing harmful content online has serious shortcomings regarding protecting principles of net neutrality and open internet. The threat of website blocking, proposed as a punitive measure for OCSP deemed noncompliant, is a direct violation of net neutrality.

Other problematic areas identified in the government's proposed regime include national security accountability and oversight, and risks to the open exchange of information and infringement of basic civil liberties. It's worth noting that net neutrality and the Charter of Rights and Freedoms are never mentioned once in the technical paper and discussion guide. The concerns highlighted in this submission need to be more fulsomely discussed with stakeholders and better nuanced to protect rights and freedoms while addressing legitimate concerns over online criminal activity.

CAUT strongly recommends more extensive consultation, including rescheduling roundtable discussions, to find a way forward to protect against discrimination, harassment, and violence, while avoiding regulating expression that may offend some, but is lawful. September 2021



Seathand construction to the first set of the first start and the set of the second set of the set of the set of the second set of the set of the set of the second set of the set of the set of the second set of the second set of the set of the second second second set of the second set of the second secon

96 Mowat Avenue Toronto, Ontario, Canada M6K 3M1

# Tucows' response to the Government proposed approach to regulating social media and combating harmful content online

#### 24 September, 2021

The ongoing Covid-19 pandemic has thrown into stark relief how important it is that Canadians have full and equitable access to the free and open Internet. With the sudden and urgent necessity to avoid in-person interaction, Canadians have turned to the Internet to do business, attend school, and socialize with other people in Canada and around the world. While addressing a true need, this broad turn towards online interactions has of course also led to an increase in exposure to harmful content online. We need standards, we need to enable safe and secure access to information and to community, and we need to protect Canadian Internet users in a fair and balanced way. We appreciate that the Government of Canada is working to address these needs.

Here at <u>Tucows</u>, we believe in the free and open Internet, allowing Canadians to share opinions and artwork, meet people from all around the world, and live our lives in the digital realm just as we do in the physical world. With that goal in mind, it is crucial to find the right balance between freedom of expression and access to ideas on the one hand and protection against illegal and harmful content on the other.

Surveillance and limitations on Canadians' expression on the Internet is unacceptable; we as Canadians must be safe to express ourselves without fear of either government censorship or being harmed by the types of content this legislation attempts to address.

As a domain name services provider and a proudly Canadian company, Tucows, both as a business and as a community of coworkers, is a crucial part of the same Internet ecosystem that we all use every day. We are pleased to be able to share our expertise in this response to the Government's proposed approach to address harmful content online.

Lawmakers must not fall into the trap of making quick decisions and implementing half-formed or ill-informed plans that will have long-term effects on the rights and freedoms of Canadian citizens. When developing broad new legislation such as this, it's crucial that the Government **consider the input of experts in the industry who have already spent years working on combatting online harms and moderating content on online platforms.** To that end, we will raise our concerns with the proposed new legislation. The Government should do everything possible to gather input from Canadians, especially Canadians already working in this space, and incorporate those insights into revisions of this draft legislation.

tucows.com

Seathards - constrained to the contract of the contract of

tucows

96 Mowat Avenue Toronto, Ontario, Canada M6K 3M1

# Applicability

The legislation would apply to "Online Communication Service Providers" (OCSPs); the limitation to services that enable communication with other users of the same service is a good start but still leaves gaps such as personal websites or blogs—does a Wordpress blog with a vibrant community of commenters fall under this definition? A personal website with a message board? The exemption for private communications is crucial and must be clear enough to preclude any surveillance of personal expression or private communications.

The five categories of harmful content being addressed here (hate speech, child sexual abuse material (CSAM), non-consensual sharing of intimate images, incitement to violence, and terrorist content) are appropriate categories, as each one poses **imminent risk of harm to a person**, and are already prohibited under the <u>Criminal Code</u>.

We also support the OCSP reporting requirements relating to harmful content and particularly note "how they monetize harmful content" as a valuable metric to track and disclose.

# **Privacy Concerns**

It is crucial to ensure that **Canadian citizens' privacy rights are not only respected but are a fundamental part of any new legislation**, especially relating to online services where personal data is essentially currency and people are highly vulnerable to the theft of their data, their money, even their identity.

How will improper and excessive surveillance and storage of personal data be prevented, especially in the case of false positives, considering the known limits and biases of algorithmic content flagging?

Relatedly, the oversight for accessing Basic Subscriber Information (BSI) through a Production Order is unclear or lacking; who authorizes these orders? Who makes sure that there are valid grounds to access personal data in relation to a suspected incident? Proper checks and balances must be put in place to protect Canadian citizens as well as people from around the world. We will want the rights of Canadians to be protected worldwide, which speaks to a need to participate as a country in international dialogue on this important legislative initiative, to ensure reciprocity in the protection of fundamental rights.

# 24-hour Responses

The requirement for OCSPs to take action within 24 hours of a user report or algorithm flag will absolutely lead to errors.

24 hours is not sufficient time to review reports, so OCSPs will either over-respond by taking down content that does not fall within the five categories of online harms, or they will

# tucows

96 Mowat Avenue Toronto, Ontario, Canada M6K 3M1

dismiss reports too quickly and miss actual harmful content in the frenzy. Which way it goes will depend on both the strength of the penalties for not taking down harmful content and the capacity of the individual OCSP to create a team dedicated to reviewing reports.

Regardless of the approach, this short response timeframe burdens Canadian Internet users as well as those of us who are seeking to protect them: either their content is taken down inappropriately and they must appeal the decision or their valid report is dismissed and the problematic content remains online, continuing to cause the very harm this legislation is attempting to prevent. Taking down content near-immediately upon complaint is not a thoughtful approach to this difficult dilemma, nor is it permissible under the Charter of Rights and Freedoms.

It also seems fairly arbitrary; **why 24 hours?** Where exactly did that number come from? Do our government and law enforcement agencies respond within 24 hours to similar types of reports, basing this on their real-life experience? No. When issues of this kind are reported, either by victims or by online service providers of all kinds, the RCMP takes days *at best* to respond, let alone prosecute the harms.

# Scope of harms

The scope of content that falls into these broad categories is unclear and apparently not yet defined, as that will be included in the full legislation; this should be open to the Canadian public to comment on. The Internet community has been working on the issue of online harms and abuse of the domain name system for years, and is still deep in the process of defining abuse; have the drafters of this legislation considered the work of those experts at all? And, have the response timeframes in place in those industries been considered when setting this 24 hour response time?

# Free expression

How will issues of freedom of expression be addressed? Facebook already takes down breastfeeding pictures and other acceptable content without oversight; this will expand to **people using the reporting system and fast takedown requirements to silence voices they disagree with**, including anti-choice people brigading health care forums. Imagine a woman posting a story of sexual assault to raise awareness and reclaim her story, only to find it taken down due to ill-meaning people reporting it as hate speech. The writer can submit an appeal, but it's adding insult to injury.

See Device - Construction for the Construction of Construction Proc. System Constructions (Construction Construction) (Construction) (Cons

# tucows

96 Mowat Avenue Toronto, Ontario, Canada M6K 3M1

## Use of Algorithms

Meaningful human review is crucial in this situation, as in other areas relating to content moderation and the response to online harms. Algorithms are imperfect, proven to <u>perpetuate</u> <u>the biases</u> of their creators and datasets, and false positives abound, resulting in the **uneven application of legal penalties to the communities this legislation purports specifically to protect.** Algorithmic content moderation, especially in relation to false positives in content moderation, is the topic of a great deal of <u>research</u> and many <u>popular articles</u>. To ignore this issue is to **willfully subject Canadian citizens to unequal treatment under the law**. Algorithms may be used to flag content for further human review but **must not be the sole arbitrator of what is permissible content on the Internet.** 

## Fragmentation of the Internet

Banning content in Canada that is still available in other countries will cause fragmentation of the Internet. Authoritarian governments have shown that controlling "their" internet and what their citizens can view only moves the content—users who still want to access "banned" content can easily use a VPN, for example, to appear to be in a different jurisdiction. This also means that **those harmed by the content**—the victim, for example, of non-consensually-shared intimate photos, **can no longer view (and report) the content while the harm to them continues unabated.** 

The limits on the requirement for ISPs to block Canadian access to certain content must be strong and clear. The underlying concept here is appropriate; CSAM and terrorist content is illegal and those laws must be enforced. That said, the definition especially of "terrorist content" has not been shared, and leaves open significant concerns of government overreach. As a domain registrar we have been called on to remove allegedly terrorism-related content from our platform, and in some cases the website in question has in fact been a journalism site (rather than one supporting the terrorist content), while in other cases it has posed as true journalism in order to spread messages of hate. The difficulty is in determining whether the content is in fact illegal and it's essential to this process that proper oversight exists. We work with Tech Against Terrorism to verify reports of terrorism-related content; are OCSPs now left on their own to make these determinations?

We receive many complaints every day from lawyers and other Internet users asking for full websites to be taken down when the issue is a mention of an individual, a single photo, or a single page on a larger website. How will the requirement to block Canadian access to content accommodate the fact that blocking by ISP may only occur at the IP or domain name level and cannot be as granular as free speech requires? Any prospective legislation will have to be much more precise about how an OCSP can order a customer to excise the offensive content or face takedown, otherwise we are trying to hit a fly with a sledgehammer.

tucows.com

# tucows

96 Mowat Avenue Toronto, Ontario, Canada M&K 3M1

**Enforcement capability is also in question**, as users can bypass an ISP's blocklists by using a VPN or DNS-over-HTTPS functionality, masking their traffic. How will the legislation address this gap, without overreach? What exactly are Canadian Internet businesses being asked to do?

## Commissioner powers and funding

It is both unfortunate and well known that the Canadian Office of the Privacy Commissioner lacks the power to levy fines or even effectively require organizations to change their behaviour; last year, Facebook ignored the findings of the OPC's investigation. How will the creation of this new Digital Safety Commissioner of Canada avoid the same problems? Why do the legislators expect that the new Commissioner's fines or other findings will be respected, when the existing ones are not?

We question the expectation that the operating budgets for the Commissioner and Recourse Council will be funded by OCSP "regulatory charges"; this is essentially a tax on some (but not all) online service providers. Costs will of course be passed on to Canadian Internet users, either in the form of payment for services or increased advertising on the platforms. On top of these costs for oversight bodies, we will already have incurred substantial costs dealing with all of the issues described above, including an expected increase in volume.

What is the expectation for OCSPs that decline to pay these costs? Currently, administrative penalties recommended by the OPC are often ignored and with no clear consequences.

## Engaging LEA and CSIS

Regarding the requirement for OCSPs to notify law enforcement and the Canadian Security Intelligence Service in some circumstances, we would support the 'imminent risk of human harm' limitation (the first of the two options presented), requiring those entities to notify law enforcement only when imminent harm is suspected.

Extending this risk of serious harm to property (instead of only to people) is a huge concern. There needs to be further consultation with Canadians in this area (as with much of the rest of this proposed legislation), because people are not property and harm to property or to property rights should never receive the same high level of protection as imminent harm to people must.

We are also concerned about privacy rights and surveillance in relation to this notification requirement, as discussed earlier.

tucows.com

# tucows

Seathanter - construction in the contract of the contract of the contract of the seather of the contract of the seather of the contract of the seather of the contract of t

96 Mowat Avenue Thronto, Ontario, Canada M6K 3M1

## Recourse and appeals

Access to recourse is unequal; a Canadian (or anyone living in Canada? It's unclear!) whose content is removed under this new law can appeal to the platform itself and then to the Digital Recourse Council, but users from the rest of the world appear to have no such recourse. What happens if *their* content is removed due to a false positive flag or report? Under this proposed legislation, the platform could refuse to consider any appeal. The Digital Recourse Council may require a platform to return the Canadian user's content, but users from elsewhere would effectively be silenced from participation in Canadian online discourse, **limiting the perspectives available to Canadians. As discussed above, there is a need for international reciprocity; consultation and international agreements will be required.** 

Timeframes for appeals must be clearly laid out so all parties—users, ISPs, and OCSPs alike—understand their options and requirements. Timeframes should be long enough to ensure that users have plenty of time to address content removals. The Recourse Council will need to be prepared for a significant volume of appeals and must be held to the same response time that OCSPs are held to—currently 24 hours.

## Recommendations

With the above comments in mind, we offer the following recommendations. We look forward to reviewing future versions of this framework before it is passed into law, and are happy to assist by providing expertise and insights at every stage of the process.

The Government should:

- 1. Launch a detailed consultation, ensuring that those working on combatting online harms play a key part in assisting to modify this draft legislation
- Work with the Privacy Commissioner of Canada and the Provincial and Territorial Commissioners to make the privacy rights of Canadian citizens a foundational element of this new legislation
- Balance the prevention of these five categories of harm against the Charter rights of Canadian citizens, protecting our privacy and freedom of expression while preventing surveillance, limitations on free expression, and the use of algorithms to silence Canadian voices
- 4. Address questions around funding for this new Government department
- Prepare the Digital Recourse Council for a significant volume of appeals and ensure they are able to respond within the same timeframe to which OCSPs are held

This comment was prepared by Sarah Wyld, with thanks to Jacinta Sandiford, Reg Levy, Graeme Bunton, and Stephanie Perrin for their input.

tucows.com

Michards, and a process of the second system of

September 24, 2021

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St Gatineau QC K1A 0S5

Dear Ministers and Members of the Digital Citizen Initiative,

We are writing as stakeholders about our concerns with the proposed Canadian legislation, and its impacts on legal adult business and sex workers.

As the nonprofit trade association for the adult industry in the United States and Canada, we are an active participant in the fight against the distribution of child sex abuse material (CSAM), non-consensual intimate imagery (NCII), and other illegal content. While many assume that adult companies are negligent if not complicit with the distribution of illegal content, actual data shows that adult platforms have led the fight, and are much more effective at preventing the distribution of illegal content than our mainstream counterparts.

Adult businesses understand both the importance of, and the challenges involved in, differentiating legal and illegal content better than almost any other stakeholder. We also understand the technology, the costs involved in implementation (both financial and social), the sometimes unintended consequences, and the potential for abuse.

While we understand that the legislation is still germinal, we are troubled by certain provisions in the existing framework that we hope to address. Of particular concern is the 24-hour removal standard for platforms informed of potentially illegal content.

Traditionally, flagging protocols produce large volumes of content for review, even though only a fractional percentage of that content ever meets the legislated definitions. While large global companies like Facebook, with 24/7 moderation staff, may be able to comply with this timeframe, smaller companies will not. This puts an undue burden on start-ups and other small businesses, and encourages outright banning of any content related to sex or sexuality.

Furthermore, with user-generated content, it may be difficult to definitively assess whether a flagged piece of content meets a legislated definition, especially within 24 hours of a report. Given the penalties, most platforms are likely to proactively remove broad swaths of content that is legal and does not meet the legislated definitions, rather than risk fines or other regulatory action for inadvertently removing something that does.

We know from experience that these types of reporting and removal requirements that are overly burdensome can lead to discriminatory censorship of marginalized communities, including LGBTQ+ people, people of color, sex workers, sex educators, and the fetish and kink communities. These communities already suffer from widespread deplatforming on social media. We fear the proposed reporting and removal requirement will accelerate and exacerbate this censorship.

While the framework does provide for an appeals process for the author and the flagger, a large percentage of social media activity and content creation is anonymous and divorced from original authorship. While the regulation is well-intentioned, this protocol provides the flagger — who may have no greater insight into the genesis or reality of a specific piece of content than the poster — an outsized voice in having legal content removed.

We see this as a particular concern for marginalized communities. Over the past two years, there has been a concerted effort from conservative, anti-porn religious groups to categorize all or most adult content as exploitative, coercive, or violent. In many cases, they do not believe that any adult content can be made consensually. They are opposed to the rights of sex workers and LGBTQ+ people. We have already seen cases of brigading — coordinated groups strategically flagging content or profiles on social media sites — in order to censor legal content they deem offensive.

For these and other reasons, we ask that you work with us as a stakeholder while developing these regulations, as we are in a unique position to help you understand the technologies and mechanisms of moderation, as well as the potential risks. We believe we can help develop more effective regulations while still protecting the rights of legal creators and marginalized communities, and look forward to hearing from you as the legislation progresses.

Sincerely,

Mike Stabile Director of Public Affairs Free Speech Coalition



#### Global Network Initiative Submission to the Government of Canada on the Proposed Approach to Addressing Harmful Content Online

#### Introduction

The Global Network Initiative (GNI) appreciates the opportunity to provide input in response to the Canadian Government's proposed <u>approach</u> to addressing harmful content online ("proposed approach"). GNI is the world's preeminent multistakeholder collaboration in support of freedom of expression and privacy in the information and communications technology (ICT) sector. GNI's members include leading academics, civil society organizations, ICT companies, and investors from across the world. All GNI members adhere to the <u>GNI</u> <u>Principles on Freedom of Expression and Privacy</u>, which provide guidance on how to navigate government demands and restrictions consistent with international human rights law and the UN Guiding Principles on Business and Human Rights.

GNI brings a unique set of perspectives and experiences to bear on the issues addressed in this consultation. Last year, GNI conducted wide-ranging research and global consultation on legal and regulatory efforts to address online harms around the world. GNI engaged in a detailed analysis of two dozen such content regulation efforts, convening six events targeting government officials and other stakeholders in <u>Africa</u>, the <u>EU</u>, <u>India</u>, <u>Pakistan</u>, and the <u>U.K</u>. This work culminated in GNI's <u>Content Regulation and Human Rights Policy Brief</u> (policy brief), which identifies helpful and problematic elements of emerging approaches and includes specific recommendations for how governments can address digital content-focused concerns consistent with human rights principles.

Our analysis of the proposed approach draws upon the diverse expertise of our multistakeholder membership and benefits from the analysis in the policy brief and our feedback on dozens of domestic content regulations in other countries. We stand ready to answer any questions and to continue to engage constructively with the Canadian government on the proposed approach and any other matters related to human rights in the digital age.

#### Analysis

#### 1. Canada's Leadership Role in Human Rights

GNI acknowledges and is grateful for the significant role the Government of Canada has played in supporting the development of an open, interoperable, safe, and secure Internet. This includes Canada's role as a founding member and upcoming chair of the Freedom Online Coalition, leadership in the work of UN bodies and other multilateral initiatives dealing with issues of Internet governance, and active engagement in various multistakeholder processes, such as the Christchurch Call to eliminate terrorist and violent extremist content online.



As a result of this prominent leadership, the approaches Canada takes to addressing concerns about online harms will serve as a reference point for other governments and contribute significantly to global norm setting. They will also impact the ability of the Canadian government, as well as other aligned governmental and non-governmental actors, to engage with and influence similar efforts in other countries.

While we appreciate the public policy rationale for addressing online harms, we are concerned that some aspects of the proposed approach appear to be inconsistent with international human rights principles, regulatory best practice, and Canada's leadership on Internet freedom. We encourage the Government of Canada and the Canadian Parliament to ensure that its efforts are fully aligned with the country's international human rights commitments and will support, rather than hinder, its continued international leadership on these matters.

#### 2. Focus on online harms

The proposed approach aims to address concerns about online harms in at least five areas — terrorist content, content that incites violence, hate speech, non-consensual sharing of intimate imagery, and child sexual exploitation content — all of which are illegal under the Canadian Criminal Code. We very much appreciate the commitment to focusing on areas of speech and conduct that are already defined in domestic law, rather than creating new and vaguely defined categories. However, we also note with concern the proposal's aim to "borrow" existing definitions and adapt them to the "regulatory context." Opening up these categories of prohibited speech to re-definition is likely to lead to significant controversy. Any changes made to these definitions are likely to confuse the public and create uncertainty, especially when it comes to use of humorous, satirical, and journalistic content, as well as counter-narrative efforts (e.g., CVE). In addition, such changes will weaken the value that existing jurisprudence can have in helping actors, including Online Content Service Providers (OCSPs), who will need to interpret and apply these categories.

It is critical that any further regulation avoid broadening the definitions of these existing provisions specifically for the online space. As we note in the policy brief, requiring removal of certain forms of speech that would otherwise be legal in analog form raises risks of discriminatory impacts and undermines the broad scope of the right to freedom of expression. The government's background paper states "the approach upholds and protects human rights, while also respecting fundamental freedoms, notably freedom of expression." However, it fails to sufficiently acknowledge the potential that overly broad definitions, particularly when paired with significant obligations on intermediaries and penalties for noncompliance, could contribute to invasive monitoring of users and unnecessary restrictions of their content and conduct. As just one example, the technical paper states that "[t]he concept of terrorist content, should refer to content that actively encourages terrorism and which is likely to result



in terrorism," which ignores further qualifications such as intent to intimidate the public and political and religious motivations that exist for definitions of terrorism in Canadian law.

#### 3. Scope of application

In the <u>policy brief</u>, we call on lawmakers and regulators to ensure any restrictions on freedom of expression imposed by content regulation efforts meet the standards of necessity and proportionality. One critical way to avoid unnecessary and disproportionate impacts on freedom of expression is to focus these approaches on those services that are best positioned to identify and address the "specific concerns at issue." In this regard, we applaud the proposal's exclusion of private communications services, as well as telecommunications companies, neither of which are well positioned to implement the proposed regime in a proportionate manner.

Furthermore, we appreciate that the technical paper proposes authorities to target specific obligations to specific categories (and sizes) of companies. However, the broad definition of OCSPs in the proposal overlooks the significant disparity in capacity for certain smaller companies and companies at different layers of the ICT stack to implement the obligations outlined in the proposal — with one expert noting a particular risk for <u>internet infrastructure</u> providers. The apparent lack of attention to and nuanced application toward new and smaller providers could create unnecessary and unintended market consequences.

#### 4. Breadth of obligations

The proposed approach presents a set of sweeping obligations for OCSPs in Canada that, as framed, could pose significant risks for freedom of expression and privacy. These obligations cover moderation practices around potential harmful content, transparency measures, reporting requirements to law enforcement and/or intelligence agencies, and related data preservation requirements.

Under the proposed approach, OCSPs "must take all reasonable measures, which can include the use of automated systems, to identify harmful content that is communicated on its OCS and that is accessible to persons in Canada, and to make that harmful content inaccessible to persons in Canada." The act calls on OSCPs to respond to reports of harmful content from any person in Canada "expeditiously" (currently defined as within 24 hours).

As we note in the policy brief, "by imposing strict time limits on all content adjudication, states may effectively hinder the ability of ICT companies to prioritize resources and make nuanced, content and circumstance-specific determinations. These time limits may also make it difficult for the author to contest the allegation (i.e., issue a counter-notice) or seek injunctive relief or other remedy." The proposed approach implies Canadian authorities could shorten or otherwise adjust timelines for the different forms of harms. We strongly encourage an alternative approach that provides clear guidance as to what characteristics or circumstances merit prioritization in content moderation and allows flexibility to those charged with making such determinations.



GNI appreciates the need for robust content moderation processes and believes that international human rights and due process standards should guide both these processes and any corresponding regulatory approach. In this regard, we are pleased to see proposed requirements for OSCPs to provide notice about decisions to their users, as well as opportunities for redress. As we note in the policy brief, however, outsourcing enforcement of criminal provisions to private companies, without appropriate guidance on interpretation and application (e.g., the lack of a clear definition of "reasonable measures"), raises significant concerns under the international principles of legality and necessity.

The current framing also encourages adoption of and reliance upon automated content filters, which are unlikely to serve as the least restrictive means to address the broad set of harms identified in the proposal. The biases that have been documented to feed into and be perpetuated by such automated measures can also undermine the stated aim to ensure that companies' moderation practices "do not result in differential treatment of any group based on a prohibited ground of discrimination within the meaning of the <u>Canadian Human Rights Act</u> and in accordance with regulations." As with other provisions, this reliance on filters, if enacted into law, is likely to be picked up upon and emulated by other governments.

The proposed approach also sets forth reporting obligations that pose significant risks for user privacy. The proposal sets out two different potential regulatory approaches requiring platforms to either (1) notify the Royal Canadian Mounted Police "where there are reasonable grounds to suspect the content within five categories reflects imminent risk of serious harm," or (2) report prescribed content to law enforcement and/or the Canadian Security Investigative Service (CSIS) "to allow for appropriate investigative and preventive action." Requiring platforms to proactively monitor and then share user data, without any sort of specific request, effectively deputizes non-democratically accountable providers as law enforcement and adds significant challenges for companies working to uphold commitments to user privacy.

As we describe in the policy brief, requirements for transparency by intermediaries and states can offer important safeguards to help mitigate the potential for over-removal and selfcensorship. We therefore appreciate the stated commitment to require enforcement bodies to issue annual reports to the Minister of Heritage, as well as to require decisions and orders from enforcement bodies to be made public. It is important that these transparency requirements are sufficiently detailed and reviewed on an ongoing basis so that government agencies and oversight bodies can adjust for rapid changes in technology and trends. Meanwhile, company transparency reporting requirements must afford sufficient flexibility to accommodate different company size and business models, and allow companies to prioritize addressing the most salient harms on their respective platforms. It is also important that the Canadian government work with partners like Australia, the European Union, and the United Kingdom, who are also considering detailed reporting requirements, to ensure consistency in approach.



#### 5. Enforcement

The proposed approach contemplates creating a series of new regulatory bodies, each with distinct roles and powers. These would be in addition to existing prosecutorial and judicial bodies, as well as others proposed in separate but complementary legislative proposals. The sheer number of new and newly empowered entities raises the possibility of both overlaps in authority and possible gaps in implementation.

Beyond these operational concerns, GNI is also worried that the proposed approach does not provide sufficient mechanisms for ensuring oversight and accountability of these bodies, including by democratically elected bodies like Parliament. As we set out in the policy brief, "[t]o the extent that substantial rulemaking authority and discretion is delegated to independent bodies, the scope of the regulator's duties and corresponding legal safeguards must be set out in primary legislation. States must create robust oversight and accountability mechanisms to ensure that those bodies act pursuant to the public interest and intervene in markets in a non-arbitrary way, consistent with the state's obligations." Transparency requirements, while laudable, are not likely to sufficiently safeguard against potential abuse or scope creep.

Of the new entities contemplated, the Digital Safety Commissioner appears to be the most formidable. The proposed approach would give significant powers to administer and enforce the proposed obligations, including a novel "complaints regime" focused exclusively on complaints of "non-compliance." While the proposal acknowledges the likelihood of complaints being received that are "trivial, frivolous, vexatious, made in bad faith," it provides no mechanism to punish or otherwise disincentivize such misuse. Without such measures, and combined with the significant penalties contemplated for non-compliance, we are concerned that this complaints mechanism could turn into a megaphone to amplify the impact of the "heckler's veto."

In addition, the proposal to empower the Commissioner to conduct inspections of OCSPs, including physically accessing "any place" or "any thing," at any time, for any reason (not to mention the contemplation of the possibility of the use of force in such inspections), is incredibly broad and inviting of abuse and should be significantly circumscribed. While audits can be a useful enforcement tool, these powers create the potential for overly intrusive and potentially coercive inspections, as well as a possible backdoor for unauthorized surveillance. There are ample examples of how such broad and unchecked authorities have been abused in other countries. In short, this aspect of the proposed approach would be an unnecessary and unfortunate precedent.

We welcome acknowledgement of the need for and resourcing of bodies such as the proposed Digital Recourse Council that can empower and educate users. The parallel "complaints regime"



set up to allow this Council to review and reverse content moderation decisions could also have some merit. While we appreciate any efforts to enhance access to remedy for individuals who feel their rights may have been violated, the proposed regime suffers from the same lack of consideration noted above about how to mitigate against abusive or inappropriate complaints. It is also important to ensure that individuals impacted by the Council's determinations will continue to have recourse to traditional judicial processes, where appropriate.

In addition, we welcome the possibility of establishing an "Advisory Board" to allow for diverse, non-governmental expert advice, but are confused by the lack of clarity in the proposal as to the specific functions contemplated for such a Board.

#### 6. Changes to the Existing Legal Framework

The proposal also suggests modifying the existing legal framework for data retention and for authorities to access data in certain circumstances. The first would amend the Mandatory Reporting Act to require reports of child pornography by covered entities to include transmission data, as well as possibly basic subscriber information (BSI), without judicial authorization. GNI appreciates the importance of addressing internet child pornography and supports collaborative efforts to identify and remove such content. Because of the proactive and mandatory nature of this reporting, GNI has concerns about the extent to which such reporting may include false positives, and therefore the impact that requiring any additional personal identifying information could have on innocent users. Of the options under consideration (to require reporting of transmission data, or to also require BSI), the former would best serve the government's stated purposes of "expediting the police response," "while respecting freedom of expression, privacy protections, and the open exchange of ideas and debate online."

The proposal also contemplates amending the Canadian Security Intelligence Service Act to allow CSIS to access BSI information held by OSCPs "more quickly" in order to "investigate and mitigate the spread of violent extremist narratives that may inspire real-world acts of violence." Lowering the legal threshold and associated due process for intelligence services to access BSI could have result in significant privacy infringements and chilling effects on expression. History illustrates that the enforcement and associated impacts of such investigations often fall disproportionately on groups who hold dissenting views, minorities, and those who are least empowered to exercise and defend their rights. Before enacting any such authorities, the government should provide clear evidence of both why such new authorities are necessary, and what additional safeguards and oversight could be effective in mitigating such concerns (beyond existing review by the National Security and Intelligence Review Agency and the National Security and Intelligence Committee of Parliamentarians).

Finally, in order to avoid extraterritorial impacts and conflicts of law, any expansions of authority to compel production of transmission data or BSI should be focused clearly and narrowly on content that has an appropriate jurisdictional nexus to Canada.

Construction of a construction of the control of Construction of According Science and According Office of Sciences and According of the According to According to According to the Construction of the Construction of According The Construction of According to Acc



GLOBAL NETWORK

GNI Submission to Government of Canada 24 September 2021

#### Conclusion

The proposed approach puts forward a vast array of new obligations on OCSPs, new enforcement bodies, and new powers and authorities. While there is no doubt that new regulatory attention and approaches are needed, the burden is on the government to make a clear case for why so much is required to be implemented so quickly. Without further articulation of both the specific challenges that the government intends to address, and clear evidence for why the proposed changes are required and well-tailored to address those, the government risks creating confusion and unintended consequences at home. It also risks undermining the critical and well-deserved reputation and influence that it has on internet policy and governance abroad.

The GNI and its members are ready to continue to engage with the government on its concerns and to work constructively to shape proportionate and effective regulatory approaches that will strengthen freedom of expression and privacy in Canada, and provide a model truly worthy of emulation by other countries.

Englande sonn to sport i contra po o EN son Passi à l'Announness Mannes (Alexa, son contra port de l'assest (Brastine) (Alexa)



#### Submission to the Department of Canadian Heritage

Consultation: The Government's proposed approach to address harmful content online

#### SUBMITTED BY: Defend Dignity

1

#### September 24<sup>th</sup>, 2021

Defend Dignity exists to end all forms of sexual exploitation in Canada. As a national organization, we have worked with survivors of sexual exploitation across Canada since 2010. We were recently appointed by the All - Party Parliamentary Group to End Human Trafficking as the first point of contact for English-speaking individuals seeking legal assistance for their victimization by Pornhub/MindGeek. We have also hosted numerous events to educate over 2,000 people in Canada and abroad on various aspects of sexual exploitation. We have developed a youth training curriculum and in May, 2021, 1,200 people attended our virtual <u>Canadian Sexual Exploitation Summit</u>, which included the participation of survivors of Child Sexual Abuse Material (CSAM) and non-consensually shared intimate images. Advocating for policies that combat sexual exploitation is another key area of our work. For example, our <u>Choose Change</u> campaign allows us to dialogue with executives from companies such as Instagram and TikTok about the need to protect children from being exposed to predators and pornography.

Our work supporting and partnering with individuals who have been sexually exploited including through CSAM and/or non-consensual material - gives us insight into the urgent need to curb online exploitation. We have witnessed the devastating impact these abuses have on victimized individuals. As our expertise is in the area of sexual exploitation, all of our recommendations outlined below will focus on addressing child sexual exploitation material and the non-consensual sharing of intimate images. These recommendations are based on specific sections of the Technical Paper and the corresponding Module number and section are indicated.

Nacional Constantin Providi de 1996 - Stan Stan Statistica de Constanti Maria de Constantino de Constantino de 1997 - Constantino de Constantino de Const 1997 - Cons

#### Recommendations

#### Module 1 (4)

We recommend extending the list of regulated entities beyond "Online Communication Service Providers (OCSPs)". There are many types of internet service providers that all play a role in making illegal content accessible to users and all should have to follow the regulations to ensure their success. The Canadian Centre for Child Protection explained the importance of legal requirements for all entities involved in the second recommendation in their report *Project Arachnid: Online Availability of Child Sexual Abuse Material*:

"All of the companies bound by these contractual arrangements are necessary to make content ultimately accessible to an end user. As a result, to address a particular problem, every entity within the system must be bound by enforceable contractual terms that address the problem and also be required to impose and enforce similar contractual terms against its own customers. If any entity in the chain is not bound by such terms, or is not willing or able to enforce its own terms against its customers, that gap can be exploited thereby enabling the problem to flourish<sup>1</sup>."

#### Module 1 (6)

It is important that this Act will apply to companies that provide services to people in Canada, as this will help prevent sites from using the jurisdiction of their physical location to avoid compliance.

#### Module 1 (8)

2

We fully support the decision to include material relating to child sexual exploitation that may not constitute a criminal offense in the concept of child sexual exploitation content. There are many related abuses that significantly harm children. The Canadian Centre for Child Protection lists several abuses that should be included as criteria for harmful content:

"A series of images, some of which were taken prior to or after the act of abuse was recorded;

Images of children in bathing suits distributed on forums dedicated to sexualizing children;

Images of children urinating;

<sup>&</sup>lt;sup>1</sup> https://protectchildren.ca/pdfs/C3P ProjectArachnidReport Summary en.pdf

Stadional and Copies and the second secon

Imagery depicting clothed or semi-clothed children in provocative poses, sometimes inaccurately labelled as "child modelling"; Images of children being physically assaulted or tortured; Information related to grooming and/or abuse tactics; Written content describing or advocating/counselling child sexual abuse; Sexual commentary related to an image or video of a child; Releasing of personal information about a child."<sup>2</sup>

We also support the concept of non-consensual sharing of intimate images including instances where it is impossible to know if all individuals depicted gave their consent. Individuals who are victimized in this way experience severe and long-lasting harms and having the content permanently removed from the internet after it has been uploaded is nearly impossible.

#### Module 1 (10)

Requiring sites to monitor the content they host is important, however there must also be robust mechanisms to verify the age and consent of all individuals depicted before any intimate content can be hosted. This is recommended in both the Canadian Centre for Child Protection's report *Project Arachnid: Online Availability of Child Sexual Abuse Material* and the Ethics committee's report *Ensuring the Protection of Privacy and Reputation on Platforms Such as Pornhub*<sup>3</sup>. The Ethics committee's report also recommends that platforms will be liable for failing to prevent the upload of CSAM or non-consensual content. Every effort must be made to stop child sexual abuse material and/or non-consensually shared images from being hosted on the internet in the first place. That will prevent the devasting and long-lasting consequences inflicted on victimized individuals. Prompt removal of this illegal content is a crucial part of the solution, but it must be used as a compliment - not replacement - to robust prevention strategies.

#### Module 1 (11)

Module 1 (11) states that sites are supposed to address flagged content within 24-hours, or a timeframe determined by the Governor in Council depending on the type of content. Given the severity of illegal sexual content, we highly recommend that sites be required to use technology

<sup>&</sup>lt;sup>2</sup> https://protectchildren.ca/pdfs/C3P ProjectArachnidReport Summary en.pdf

<sup>&</sup>lt;sup>3</sup> <u>https://www.ourcommons.ca/Content/Committee/432/ETHI/Reports/RP11148202/ethirp03/ethirp03-e.pdf</u> and https://protectchildren.ca/pdfs/C3P\_ProjectArachnidReport\_Summary\_en.pdf

that automatically suspends access the moment this type of content is flagged, preventing its spread across the internet while it is awaiting assessment. This prioritizes the victimized individuals who are experiencing trauma from the discovery of this content.

In addition, this framework often uses the term "inaccessible to persons in Canada," such as in this section where it is describing the action sites must take to address harmful content. This could be necessary for the more subjective harms, for example the definition of "hate speech" may differ from nation to nation. However, there is broad international consensus that child sexual exploitation content is an egregious crime. Distributing intimate images without the depicted individuals' consent is also a more objective illegal activity. We strongly advocate for entities to be required to remove child sexual abuse material and/or intimate images shared without consent. It is unfathomable for a victim of CSAM or non-consensual material to have to live with the trauma of knowing the depiction of their abuse is available in other countries such as the United States. Later in the Technical Paper, Module 1 (120) uses the term "removing the following harmful content." We recommend consistently using the term "removal" or "deletion" instead of "inaccessible to persons in Canada" when describing a companies' requirement to dealing with child sexual exploitation content and/or non-consensually shared material. This is consistent with the first recommendation of the Ethics committee's report Ensuring the Protection of Privacy and Reputation on Platforms Such as Pornhub<sup>4</sup> and the Australian eSafety Commissioner's website<sup>5</sup>.

Finally, if sites are given the responsibility of responding to content flagged on their services, there must be strong enforcement to ensure they follow best practices and assist survivors. In response to the testimony of victims sharing how difficult it was to try to get Pornhub to remove the material of their abuse, the Ethics committee recommended victims of non-consensually shared material be given the right to have the content removed immediately<sup>6</sup>. If a person says they did not consent or are revoking their consent, the content should be categorized as harmful and automatically removed. Likewise, if someone alerts the site that any of the individuals depicted are minors, the removal and reporting protocol should be followed immediately.

#### Module 1 (14)

Requiring entities to regularly report data to the Digital Safety Commissioner is a good step, especially the inclusion of how they monetize harmful content.

<sup>&</sup>lt;sup>4</sup> https://www.ourcommons.ca/Content/Committee/432/ETHI/Reports/RP11148202/ethirp03/ethirp03-e.pdf

<sup>&</sup>lt;sup>5</sup> https://www.esafety.gov.au/report/illegal-harmful-content/the-actions-we-can-take

<sup>&</sup>lt;sup>6</sup> https://www.ourcommons.ca/Content/Committee/432/ETHI/Reports/RP11148202/ethirp03/ethirp03-e.pdf

Machanika construction of a statistical statistical statistical construction construction of statistical statistical statistical statistics.

#### Module 1 (17)

If the Digital Safety Commissioner is granted the ability to tailor regulations, there must be limitations on that authority to ensure that there will be zero-tolerance for CSAM and nonconsensually shared intimate images regardless of differing business models or capacity.

#### Module 1 (20)

Due to the seriousness of CSAM (it is the documentation of child abuse), we strongly recommend choosing the second option for entities' requirements to report harmful content to authorities. The first option only requires entities to report content if there is an imminent risk of serious harm. If that option is chosen, the Act should explicitly state that CSAM is always required to be reported under the *Mandatory Reporting Act* to avoid any confusion. This could be included in Module 1 (21). In Module 1 (21), it is reasonable that reporting in compliance with domestic legislation (for example *the Mandatory Reporting Act*) fulfills the obligations set out in Module 1 (20). However, there should careful consideration of if or in what circumstances foreign legislation could fulfill the reporting requirement.

#### Module 1 (23)

We strongly support requiring sites to preserve information related to the reports that they submit to authorities and potentially illegal content.

#### Module 1 (31)

Sites should not automatically receive immunity from civil and criminal proceedings for their participation in illegal activities. If immunity is to be considered as an option, at the very least there should be robust criteria a site must meet before it could be eligible to receive it. Regulation is one tool to curb online harms, however it should be a layer of protection that compliments – not diminishes - civil and criminal liability. Victimized individuals should have the right to pursue justice and offending sites should be held accountable for their actions.

#### Module 1 (54-55)

5

There should be limits on the Digital Recourse Council of Canada's authority to determine whether content is harmful for some categories. Specifically, CSAM should always be classified as harmful, and the benefit of the doubt should apply for instances of non-consensually shared intimate images. Furthermore, if an individual initially gave their consent, they should have the ability to revoke their consent and have the content removed.

#### Module 1 (110)

There should be great caution in allowing due diligence to be a defense from an alleged violation. It can be difficult to confirm the presence of a mental element, and this could be used to avoid compliance. The Act must ensure it is robust enough to hold sites accountable.

#### Module 1 (94 and 120)

Under our suggestion for Module 1 (10) we discussed the importance of requiring sites to verify the age and consent of all individuals depicted before uploading sexually explicit material. The Act should include the failure to prevent the uploading of CSAM and/or non-consensually shared images in the list of violations in Module 1 (94). In addition, a site that persistently hosts child sexual exploitation content should be considered for the exceptional recourse measures outlined in Module 1 (120). There needs to be sufficient liability to stop sites from distributing CSAM.

#### Module 2

We are pleased that the new framework includes strengthening the *Mandatory Reporting Act*. Many of the suggested amendments will enhance efforts to curb CSAM. We strongly advocate to adopt Module 2 (8), which would require companies to include basic subscriber information in their reports to law enforcement. This prioritizes protecting children by allowing law enforcement to locate offenders faster.

#### Additional Recommendation

Creating a framework to address online harms provides an opportunity to protect children in a couple of ways. We are pleased that curbing CSAM is a key focus of this new legislation and we would like to suggest another step to prioritize children's safety. Sites that host sexually explicit content should be required to verify the age of their consumers to protect children and youth from being exposed. In June 2021, the Senate passed *Bill S-203: An Act to restrict young persons' online access to sexually explicit material*<sup>7</sup> and it was sent to the House of Commons for the next stage of the legislative process before the election. The Senate recognized the urgency of preventing the various harms associated with youth's exposure to pornography, and many national and international authorities agree. For example, the Canadian Centre for Child Protection recommended age verification in their report to combat CSAM<sup>8</sup> and Australia's eSafety Commissioner is developing a plan to implement age verification<sup>9</sup>. Canada's Digital

<sup>&</sup>lt;sup>7</sup> https://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E&billId=10873545

<sup>&</sup>lt;sup>8</sup> https://protectchildren.ca/pdfs/C3P ProjectArachnidReport Summary en.pdf

<sup>&</sup>lt;sup>9</sup> https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification

Safety Commissioner should include mandatory age verification for sites that host sexually explicit content in its regulations.

Thank you for recognizing the severity of this matter and for working to create a robust framework to combat online harms. We would be happy to connect with you as you continue to work on this crucial initiative.

Submitted by: Jenna Scholz, Defend Dignity's Coordinator of Research and Government Advocacy jenna.scholz@cmacan.org 416-674-7878 Ext 243

Defend Dignity 101- 2580 Matheson Blvd. E. Mississauga, ON, L4W 4J1

Land of the Mississaugas of the Credit First Nation

Discharding and a perturbative process of the test of the second se

## The Government's proposed approach to address harmful content online

Global Partners Digital submission September 2021

#### About Global Partners Digital

Global Partners Digital is a social purpose company dedicated to fostering a digital environment underpinned by human rights.

#### Introduction

We welcome the opportunity to provide comments on the Canadian government's proposed approach to address harmful content online through a new Act of Parliament. GPD recognises the legitimate desire of the government to tackle harmful content online, and many of the proposals put forward in the discussion guide and technical paper are reasonable and sensible. Based on our analysis, however, we believe that particular aspects of the proposal, if taken forward in their current form, may pose risks to individuals' right to freedom of expression and privacy online and could be inconsistent with Canada's international human rights obligations.

In this response, we relay our concerns and make a series of recommendations on how the proposal could be revised to mitigate these risks. We believe these considerations and recommendations, if incorporated into the upcoming legislation, will help safeguard freedom of expression and privacy online.

#### Framework for analysis of the proposed approach

Our analysis of the government's proposed approach is based on international human rights law, specifically the International Covenant on Civil and Political Rights (ICCPR), ratified by Canada in 1976. Article 19 of the ICCPR guarantees the right to freedom of expression, including the right to receive and impart information and ideas of all kinds regardless of frontiers. Article 17 of the ICCPR guarantees the right to privacy and provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence". Restrictions on the right to freedom of expression or privacy guaranteed under international human rights law are only permissible when they can be justified. In order to be justified, restrictions must meet a three-part test, namely that: (1) restrictions are provided by law; (2) restrictions pursue a legitimate aim; and (3) restrictions must be necessary and proportionate, which requires that the restriction be the least restrictive means required to achieve the purported aim.

It is important to remember that Canada's obligation to ensure that these rights are not unjustifiably restricted exists both in relation to restrictions which stem from the actions of the state itself as well as those caused by third parties, such as private companies. As such, it makes no difference from the perspective of the individual affected whether any restrictions are imposed and enforced directly by the state (e.g. through creating criminal offences which are enforced by the police and the courts) or through third parties, particularly when the third party is acting in order to comply with legal obligations.

1

Human rights analysis of the proposed approach

#### **Scope of Entities**

We are concerned about the scope of entities included under the proposed framework. The technical paper sets out that new rules and obligations would apply to all Online Communication Service Providers (OCSPs), and defines Online Communication Services (OCSs) as "a service that is accessible to persons in Canada, the primary purpose of which is to enable users of the service to communicate with other users of the service, over the internet". While this would exclude some online services, the proposal would still include a broad range of entities, of all sizes, without providing a clear list of determining or limiting factors. Notwithstanding the current definitions and exemptions, we recommend that the government be required to consider a range of criteria and use these to designate entities on this basis *before* they would become subject to any regulatory requirements.

This would ensure the scope of entities subject to the regulatory requirements would be more proportionate. Were all entities falling within the definition of OCSPs to be bound by those requirements, this would not constitute a narrowly tailored and proportionate response, and would place an unreasonable regulatory burden upon smaller entities. We are concerned that higher regulatory burdens will reduce competition in the market, and power may be further concentrated on a smaller group of large online platforms. This would lead to fewer places for individuals to express themselves online and ultimately affect freedom of expression in the aggregate.

We therefore recommend that the proposal include certain factors which the government would be required to consider when making determinations on entities within scope. This should include the varying size (based on the number of users and resources) and nature of services, and include only those where there is compelling evidence or rationale necessitating their inclusion. While the language in the proposal requiring the government to consider whether there is "a significant risk that harmful content is being communicated on a particular entity" (albeit only in relation to further inclusions or exclusions of services) meets this standard in part, we recommend that it be further developed in line with the above, and also to include explicit consideration of users' rights to freedom of expression and privacy.

This would bring the proposal in line with the approach taken by other states. For example, Ireland's Online Safety & Media Regulation Bill provides that online services within scope will be designated by a newly created Media Commission. The Bill Includes explicit exemptions for certain types of services, and requires the Commission to have regard to the nature and scale of services, and the fundamental rights of users and operators, among other factors, when making designations. It would also provide services with the ability to appeal designations in court. These provisions would serve as a substantive check against inappropriate designations and reflect a proportionate and clear risk-based approach.

While we recognise - and welcome - the fact that the Digital Safety Commissioner would be authorised to tailor regulatory requirements to different categories of OCSPs, and that this would take into account different business models, sizes and resources, it is not clear how much discretion there will be tailor requirements given that many of those set out in the proposal are quite prescriptive. In addition to the Digital Safety Commission being able to tailor requirements, we believe that consideration of whether any regulatory requirements should be imposed at all is also necessary and that this should be undertaken when designating categories or OCSPs as bound by the legislation in the first place. **Recommendation 1**: We recommend that the government be required to consider a range of criteria and to use these to designate entities on this basis *before* they would become subject to any regulatory requirements.

**Recommendation 2**: We recommend these criteria include consideration of the varying size of entities (based on the number of users and resources) and nature of services, and include only those where there is compelling evidence or rationale necessitating their inclusion. We further recommend that these criteria include a specific requirement to consider users' rights to freedom of expression and privacy.

The process for excluding or including new categories of services is also troubling as it provides the government with the ability to expand the scope of entities without sufficient parliamentary oversight. The proposal simply requires the Governor in Council to consult with the Digital Safety Commissioner and be "satisfied that there is a significant risk that harmful content is being communicated on the category of services or that specifying the category of services would further the objectives of this Act". We recommend that the proposal provide that the inclusion of new categories of services be subject to parliamentary approval, in the form of primary legislation.

**Recommendation 3**: The proposal should require that any changes to the types of entities within scope be done via primary legislation, as opposed to secondary legislation produced by the Governor in Council.

#### **Private Communications Services**

We are pleased that the proposal includes an exemption for services "that enable persons to engage only in private communications". However, we are concerned that this exception could ultimately include certain channels which should be considered private without additional clarification on what exactly constitutes "private communications". For example, it is not clear whether it covers large chat groups, forwarded or widely shared communications, or services with multiple functions including private communications.

The potential inclusion of private communications services is particularly concerning since many such channels use end-to-end encryption, limiting (although not eliminating) the ability of those who provide such services to filter or monitor content which is generated or shared using them. The application of any such requirements would be unfeasible unless those channels ceased to use end-to-end encryption, which would amount to an unjustifiable restriction on the right to privacy and freedom of expression.

We therefore suggest that the proposal includes additional references to individuals' right to communicate privately, including on encrypted services. Private communications services should continue to remain entirely outside the regulatory framework, and there should be additional clarification on what exactly constitutes "private communications".

**Recommendation 4**: The proposal should include additional references to individuals' right to communicate privately, including on encrypted services. Private communications services should continue to remain entirely outside the regulatory framework, and there should be additional clarification on what exactly constitutes "private communications".

#### New Rules and Obligations

We are concerned about the approach taken under the proposal, which would require that all OCSPs abide by a broad range of new rules and obligations with little clarity on how much discretion the Digital Safety Commissioner would have to tailor requirements for different categories of OCSPs. While we are pleased that some obligations, such as those on establishing appeals mechanisms and transparency requirements, would apply to all entities, compliance with some of the obligations included under the proposal would require even the most well-resourced entities to take actions which pose risks to human rights.

#### • 24 Hour Determinations

We are particularly concerned that the proposal would require entities in scope to make a determination on the legality of content within 24 hours of the content being flagged, and to then remove the content if deemed to be illegal. While we recognise that entities within scope would have the ability to decide to keep the content up, it is important to remember the context in which this legislation is being adopted, namely a concern of the government that not enough harmful content is being removed. While the letter of the law may not pressure entities to remove more content, broader political and public pressure may do so, creating risks to individuals' right to freedom of expression due to the incentive for entities to err on the side of caution or "play it safe" and remove legal content in questionable situations.

Even entities that are making their best efforts to comply with this obligation and are able to withstand any external pressure may nonetheless, due to the strict time constraints, make decisions on a rushed basis without being informed by adequate expertise. This could lead to both over-removal and under-removal, with over-removal constituting an interference with the right to freedom of expression. Moreover, this type of obligation places a potentially large financial and logistical burden on entities who are responsible for making legal determinations without sufficient expertise, and we reiterate the concerns expressed above in relation to further concentration of the market.

Recent efforts at online platform regulation have tended to promote the privatisation of law enforcement, which, as noted above, pose heightened risks for freedom of expression when content is not clearly defined, or when removals are mandated under strict timelines. We therefore recommend that this obligation be amended, and that the proposal not require online platforms to make determinations on the legality of content, and certainly not within a strict 24 hour time period. Such decisions should instead be made by public authorities with sufficient safeguards and accountability.

The risks of this approach is clearly exemplified by Germany's Network Enforcement Act (NetzDG), which requires social media networks with over two million users to establish user complaint mechanisms and remove or block access to "manifestly illegal" content within 24 hours of receiving a complaint. All other illegal content must be taken down within seven days. This law has been criticised for outsourcing legal adjudications to private entities and the over removal of permissible content.<sup>1</sup> Even the world's largest online platforms, such as Facebook, struggle to comply with this law. Facebook's July 2021 NetzDG Transparency Report demonstrates that, of all the reports in the first half of 2021 that led to a block or deletion, the company was unable to make a decision within 24 hours for several thousand cases, despite the fact that Facebook

<sup>&</sup>lt;sup>1</sup> Human Rights Watch, "Germany: Flawed Social Media Law - NetzDG is Wrong Response to Online Abuse", (2018), available at: <u>https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law</u>

employs 129 individuals to process NetzDG reports.<sup>2</sup> As the government's proposal currently sets out an even more restrictive time period (24 hours for all five types of content) it is unlikely that even the largest online platforms will be able to comply with this obligation in a way which does not present heightened risks for freedom of expression. Other proposals, such as the UK's Draft Online Safety Bill, take a tiered approach to imposing obligations, and do not provide a specific time period for the removal of illegal content.

Ideally, there would be no requirement to make determinations and take action within the proposed 24 hour time period. However, if entities are still required to make such determinations, we recommend that the proposal be amended to provide both large and small entities with a more flexible time frame when they are unable to comply with the 24 hour requirement. They should also be able to seek assistance from the government if they are unable to develop the necessary internal structures to be able to comply without posing risks to individuals' right to freedom of expression online.

**Recommendation 5**: The proposal should be amended to remove the requirement that entities make determinations within 24 hours and remove content identified as illegal. If the proposal is to include these obligations, it should, at minimum, provide entities with a more flexible time period to make determinations, and enable entities to seek assistance from the government if they are unable to develop the necessary internal structures to be able to comply without posing risks to individuals' right to freedom of expression online.

The proposal should also explore means of balancing the risks of over removal associated with time-sensitive takedowns. For example, a study exploring the optimisation of takedown and appeals processes related to content governance decisions recommends the introduction of an "Alternative Dispute Resolution Panel", in which a platform must compensate the user and cover the costs of the appeals process in the case of wrongful takedown and thus is incentivised to reduce the prevalence of over-blocking.<sup>3</sup> The proposal should also take into account the existence of additional and pre-emptive means of addressing the proliferation of harmful content online as well as removal; for example, Moonshot's research on potential interventions for 'incel' content in Canada indicates that re-directing offending users to helplines and support services, safeguarding algorithm designs to ensure that harmful content is not promoted in the feeds of vulnerable or impressionable users, and adequate prevention funding can reduce the incidence of incel-related hate speech and incitement to violence online.<sup>4</sup> These pre-emptive approaches avoid forcing offending users to migrate to smaller, less well-regulated platforms to spread the same content after it is removed or they are de-platformed elsewhere. Rather than focus solely on content removal, the proposal should include a broader range of provisions for the deprioritisation and prevention of harmful content beyond simply removing it ex post,<sup>5</sup> encouraging OCSPs to develop systems and processes which will tackle the issue in a more nuanced and rightsrespecting manner.

<sup>&</sup>lt;sup>2</sup> Facebook, NetzDG Transparency Report (July 2021), available at: <u>https://about.fb.com/de/wp-content/uploads/sites/10/2021/07/Facebook-NetzDG-Transparency-Report-July-2021.pdf</u>

<sup>&</sup>lt;sup>3</sup> Lenka Fiala and Martin Husovec, "Using Experimental Evidence to Design Optimal Notice and Takedown Process", (2018) Connecticut Law Review 50(2), available at:

https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3218286

<sup>&</sup>lt;sup>4</sup> Moonshot, Understanding and Preventing Incel Violence in Canada, (2021) available at:

https://moonshotteam.com/preventing-incel-violence-in-canada/

<sup>&</sup>lt;sup>5</sup> Evelyn Douek, "Facebook's Oversight Board; Move Fast with Stable Infrastructure and Humility", (2019) North Carolina Journal of law & Technology 21(2), pp. 42-43, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3365358

**Recommendation 6**: We recommend that the proposal include alternative means of addressing the proliferation and removal of harmful content online without resorting to the private adjudication of law enforcement and mandating that online platforms make determinations on the legality of content. Alternative approaches should emphasise the role of de-prioritisation and intervention as effective means of addressing the spread of illegal content online in a more proportionate fashion.

#### Automated Processes

We are concerned that the proposal would require entities within scope to monitor for the five categories of harmful content on their services, including through the use of automated systems based on algorithms. Given the scale of content which is generated and shared online, entities will increasingly turn to automated processes, including AI, to meet their obligations. Larger platforms tend to develop their own bespoke tools with state of the art AI research, whereas smaller platforms may have to purchase or license generic tools for adaptation to their platform. However, the risk of encouraging or mandating the use of AI is that automated processes will detect and remove content that is not actually unlawful or harmful in a particular context.

Automated processes have had some success in relation to content moderation with types of images, including the ability to scan for copies of images that have already been identified by humans as constituting child sexual abuse and exploitation. But automated processing has been less effective at interpreting speech or less specific forms of unlawful or harmful content. For example, hate speech, incitement to violence and terrorist content may be a mixture of audio, visual and text content, and may be shared for a variety of reasons (including for journalistic or research purposes). Automated processes for their detection thus rely on a combination of natural language processing, image recognition and contextual knowledge-mapping for detection, technologies which, at present, are somewhat limited; for example, most natural language processing applications have about 80% accuracy even in their trained domain where relevant contextual knowledge is built in.6 These automated technologies struggle with novel content and novel domains and with inferring users' intentions through context; for example, blacklisting particular words associated with hate speech results in the erroneous removal of commentary, testimony and satire. There is, therefore, a substantial risk that relying upon automated processes for all five forms of content will result in the removal of content which is entirely permissible due to algorithmic error.

We are also concerned that this obligation will result in discriminatory implementation, posing risks to individuals' right to non-discrimination. The proposal does provide that entities in scope must take measures to ensure that "the implementation and operation of the procedures, practices, rules and systems, including any automated decision making ... do not result in differential treatment of any group based on a prohibited ground of discrimination within the meaning of the Canadian Human Rights Act and in accordance with regulations".

However, algorithmic bias is well documented, due either to the availability of particular types of data for training the algorithm, the types of value judgements used to tag that data for training, or the biases and blind spots of those developing and testing the tool. Using automated tools inevitably results in over-censorship and/or unequal protection against online abuse of particular communities; for example, hate speech classifiers trained on widely used datasets of

<sup>&</sup>lt;sup>6</sup> See, for example, Center for Democracy & Technology, "Mixed Messages? The Limits of Automated Social Media Content Analysis", (November 2017), available at:

https://cdt.org/insights/mixed-messages-the-limits-of-automated-social-media-content-analysis/

hate speech were shown to be up to two times more likely to label tweets by African-American as offensive compared to other users.<sup>7</sup>

We therefore recommend that the proposal exclude any obligations which require or encourage entities to use automated processes to proactively monitor and remove content. The proposal should specify that, if the OCSP implements automated decision-making to meet obligations, it must ensure the use of open source tools, transparency around standards, and appropriate appeals mechanisms. Beyond these, we believe the proposal might be strengthened by reference to the sorts of safeguards that entities must implement if they choose to build or use automated tools for content flagging, such as the building in of human moderator oversight, the transparent publication of the accuracy metrics of the tools employed, and the careful evaluation of accuracy scores against the human rights risks of particular errors through expert consultation and testing prior to roll out. The proposal could be further improved by requiring robust impact assessments of AI tools - specifically with regard to bias - to assess whether entities' use of automated processes results in, or could result in, differential treatment of any group based on a prohibited ground of discrimination within the meaning of the Canadian Human Rights Act or under Article 26 of the International Covenant on Civil and Political Rights.

**Recommendation 7**: The proposal should include explicit recognition of Canada's obligation to uphold the right to non-discrimination under international human rights law, in addition to further guarantees of this right under the domestic legal framework.

**Recommendation 8**: The proposal should not compel or incentivise the use of automated processes to proactively monitor and remove harmful content, which has been proven to result in the removal of lawful and legitimate content online. If automated processes, such as those used for content flagging, are undertaken by entities to comply with obligations, these automated tools must be rigorously tested prior to roll-out through expert consultation and trials, must be accompanied by human oversight and adequate appeals mechanisms, and be regularly assessed for their impacts on users' human rights.

**Recommendation 9**: We recommend the proposal require robust impact assessments of AI tools - specifically with regard to bias - to assess whether entities use of automated processes does not result in differential treatment of any group based on a prohibited ground of discrimination within the meaning of the Canadian Human Rights Act or under Article 26 of the International Covenant on Civil and Political Rights.

#### Reporting and Preservation Obligations

We are especially concerned that the proposal would require entities in scope to either: (1) notify the Royal Canadian Mounted Police (RCMP) in circumstances where the OCSP has reasonable grounds to suspect that content falling within the five categories of regulated harmful content reflects an imminent risk of serious harm to any person or to property; or (2) report prescribed information in respect of prescribed criminal offences falling within the five categories of regulated harmful content to prescribed law enforcement officers or agencies. In addition, we are concerned that regulated entities would be required to preserve prescribed information that could support an investigation when sought by lawful means.

7

<sup>&</sup>lt;sup>7</sup> Maarten Sap & Al, "The Risk of Racial Bias in Hate Speech Detection" Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics (2019), available at: https://homes.cs.washington.edu/~msap/pdfs/sap2019risk.pdf

This is because these requirements pose a significant risk to individuals' right to privacy and could have a chilling effect on freedom of expression, particularly for marginalised groups which are already subject to the discriminatory impacts of mass surveillance and policing.<sup>8</sup> The proposal would expand the legal and technical surveillance capabilities of the state using safety as a rhetoric, but fails to establish the necessity of such obligations for all forms of content and does not devise them in a proportionate manner. We understand the government's desire to include mechanisms for engaging law enforcement and the Canadian Security Intelligence Service (CSIS), but the approach of the proposal should ultimately be to hold platforms accountable in a way that mitigates risks to privacy and freedom of expression.

We therefore recommend that these reporting and preservation obligations be removed from the proposal unless the government is able to substantiate the necessity of these obligations for each type of content. If these obligations are still included for certain forms of content, such as for child sexual exploitation content or terrorist content, then the exact circumstances for the triggering of such activity must be clearly provided for in the proposal, and must ensure that content which is flagged as illegal by an automatic tool is reviewed by a human moderator before such a process takes place, given the potential for AI error. It must further provide limitations on the types of information required and clear safeguards should be put in place around the deletion of user data if the content in question is later deemed not to be illegal.

These concerns are supported by Google and its subsidiary Youtube's challenge to new obligations under Germany's NetzDG. New obligations under will require companies to proactively and automatically pass on user data to the Federal Criminal Police Office (BKA) if platforms assume a violation of certain criminal offenses. But Google maintains that these obligations constitute a massive interference with users privacy as only 60% of the content that would be mandatorily passed on to law enforcement would contain any criminal content, resulting in the data of innocent users being permanently stored in police databases.<sup>9</sup>

**Recommendation 10**: The proposal should exclude reporting and preservation requirements unless they are able to establish the necessity of such obligations for all forms of content and devise them in a proportionate manner.

**Recommendation 11**: If reporting and preservations obligations are still included for certain forms of content, then the exact circumstances for the triggering of such activity must be clearly provided for in the proposal. It must further provide limitations on the types of information required and clear safeguards for the deletion of user data when content in question is later deemed not to be illegal.

#### **Establishment of New Regulators**

We are pleased that the proposal envisions the establishment of new regulators whose functions relate, in part, to the protection of human rights. For example, the technical paper notes that the Digital Safety Commissioner would oversee and improve online content moderation through engagement and by considering "the needs of and barriers faced by groups disproportionately affected by harmful online content such as women and girls, Indigenous Peoples, members of

<sup>&</sup>lt;sup>8</sup> Cynthia Khoo, "Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence" LEAF (2021), pp. 206-208, available at: <u>https://www.leaf.ca/wpcontent/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf</u>

<sup>&</sup>lt;sup>9</sup> Sabine Frank, "On the Extended Network Enforcement Law in Germany - Comments from Youtube", YouTube Official Blog (July 2021), available at: <u>https://blog.youtube/intl/de-de/news-and-events/zum-</u> erweiterten-netzwerkdurchsetzungsgesetz-deutschland/

racialized communities and religious minorities and of LGBTQ2 and gender-diverse communities and persons with disabilities". It also states that the Digital Safety Commission, Digital Safety Commissioner, and Digital Recourse Council would all be subject to the Access to Information Act and the Privacy Act.

However, we are concerned that the proposal lacks a clear human rights mandate for its regulators. The technical paper fails to directly reference the right to freedom of expression under both domestic and international human rights law. We believe the inclusion of these protections and explicit acknowledgement of Canada's obligations under international human rights law to be critical here given the potential negative impacts on freedom of expression and privacy posed by the proposal. We recommend that the proposal be amended to explicitly reference Canada's obligation to uphold the right to freedom of expression and privacy as enshrined under Articles 19 and 17 of the International Covenant on Civil and Political Rights, which would ensure that protecting and respecting the rights to freedom of expression and privacy is one of the regulator's statutory duties.

**Recommendation 12**: We recommend that the proposal be amended to explicitly reference Canada's obligation to uphold the right to freedom of expression and privacy under Articles 19 and 17 of the International Covenant on Civil and Political Rights, which would ensure that protecting and respecting the rights to freedom of expression and privacy is one of the regulator's statutory duties.

It is equally important that the new regulators have a dedicated staff with sufficient knowledge and human rights expertise to effectively meet the proposed functions. The Digital Recourse Council will need to make informed decisions that could potentially encroach or infringe upon freedom of expression, particularly when issuing orders to OCSPs to make content inaccessible in Canada. We recommend that these decisions, as with those made by the Digital Safety Commissioner, be made according to clear criteria that require a consideration of freedom of expression.

**Recommendation 13**: We recommend that the proposal include a requirement for the new regulators to have a dedicated staff with sufficient knowledge and human rights expertise to meet the proposed functions, and to seek external advice when necessary to carry out their respective functions. We further recommend that the proposal require the Digital Safety Commissioner and Digital Recourse Council to make decisions according to clear criteria which includes the consideration of the impacts on freedom of expression.

#### **Regulatory Powers & Enforcement**

We are particularly concerned about the sweeping regulatory and enforcement powers that would be provided to the new regulators under the proposal. For example, the technical paper states that the Digital Safety Commissioner may, by order, require an OCSP to do any act or thing, or refrain from doing anything necessary to ensure compliance with any obligations imposed on the OCSP. The technical paper includes further investigatory powers for the Digital Safety Commissioner to conduct inspections of OCSPs at any time. The Commissioner would also be able to apply to Federal Court for an order requiring Telecommunications Service Providers to block access to services which consistently fail to apply to removal orders for child sexual exploitation content or terrorist content.

Given the broad powers envisioned under the proposal, we stress the need for effective oversight, transparency and readily accessible appeals mechanisms for services to challenge decisions of the new regulators. We understand that the new regulators must have sufficient inspection and

enforcement powers to effectively carry out its functions, but are nonetheless concerned that there are limited safeguards for the exercise of these powers. We welcome those elements of the technical paper which do provide for some degree of oversight, such as the fact that compliance orders may be appealed to the Personal Information and Data Protection Tribunal, but believe that these safeguards should go further.

We recommend the inspection powers of the Digital Safety Commissioner be limited in scope and subject to procedural safeguards, enabling entities to challenge the use of these inspection powers when undertaken for illegitimate purposes or when utilised in a disproportionate manner. We further recommend that any regulations concerning the Commissioner's ability to seek orders for the blocking of services list specific criteria and thresholds for the Commissioner to consider, including a requirement that the Commissioner consider the risks to freedom of expression before applying to the Federal Court. We welcome that the technical paper would require the Commissioner to consider the level of non-compliance and potential effects of the order, such as excessive blocking, when seeking an order. However, we believe that a more specific consideration of the human rights impacts would be preferable and ensure a more proportionate approach and limit risks to freedom of expression.

**Recommendation 14**: We recommend that the inspection powers of the Digital Safety Commissioner be limited in scope and subject to procedural safeguards, enabling entities to challenge the use of inspection powers.

**Recommendation 15**: We recommend that any regulations concerning the Commissioner's ability to seek orders for the blocking of services list specific criteria or thresholds for the Commissioner to consider before applying to the Federal Court for a blocking order. This should include a clear requirement of the Commissioner to consider the risks to freedom of expression.

lacument communique, en winte de s Lot sur l'accès à l'initianneur Recoment (execusio nor commo recocecto to hinarmation dis

The Government's proposed approach to address harmful content online

> Brief submitted by the

**Canadian Association of Research Libraries** 

September 2021



www.carl-abrc.ca

(becamming commany in a mining or (a (24) sur faceby 3 (minimum) Opennisht reserved commany 2 the access to manimum lars

## **Table of Contents**

Int	roduction	2
Ap	proaches for combating online harm and misinformation that would not requ	ire
leg	islative or regulatory change	2
1.	Increasing funding for libraries	2
2.	Curtail monopolistic social media platforms	4
Co	mmentary on the Discussion Guide and the Technical Paper	5
3.	Penalties for non-compliance	5
4.	Guarding against the over-removal of content	5
5.	Expected Effects on Marginalized Communities	7
6.	Potential impact of new regulators and dependance on law enforcement	8
Co	nclusion	9

Page 1

Standburger, and standards for the scaling of relation for the standards and the scale of the

## Introduction

The Canadian Association of Research Libraries (CARL) would like to thank the Government of Canada for consulting with Canadians on the Government's proposed approach to regulating social media and combating harmful content online. The information provided in this brief reflects many of CARL's positions already submitted to governments in our Brief to the Federal Government on Access to Information Review<sup>1</sup>, Brief to the Ontario Government's consultation Trustworthy Artificial Intelligence (AI) Framework<sup>2</sup>, CARL Submission to the Office of the Privacy Commissioner's Consultation on the OPC's Proposals for ensuring appropriate regulation of artificial intelligence.<sup>3</sup>

Canadian research libraries support the assertion in the Discussion Guide that Canadian citizens deserve a "safe, inclusive, and open online environment" but we have concerns that the proposed approach may do more harm than good in many instances. First, we outline approaches for combating online harm that would benefit Canadians either in lieu or in conjunction with legislative or regulatory changes. Second, we provide commentary on the discussion guide and the technical paper.

We suggest that an important part of this process would be for the government to engage with focus groups or panel discussions composed of the many experts who have researched and published on the topic of hate speech to obtain the expert guidance that is needed moving forward.

# Approaches for combating online harm and misinformation that would not require legislative or regulatory change.

#### 1. Increasing funding for libraries

Libraries are committed to fighting misinformation online. Advocates<sup>4</sup>, researchers<sup>5</sup>, and journalists<sup>6</sup> have called on us for help, pointing to our information-seeking skills<sup>7</sup>

Access To Information - Broadening the Openness of Government, August 2021 https://www.carl-abrc.ca/wpcontent/uploads/2021/08/2021\_CARL\_Brief\_ATI\_Consultation.pdf

<sup>&</sup>lt;sup>2</sup> Letter to John Roberts, Chief Privacy Officer and Archivist of Ontario, and Chief Information Security Officer https://www.carl-abrc.ca/wp-content/uploads/2021/06/CARL\_Ontario\_Al\_Submission.pdf

<sup>&</sup>lt;sup>3</sup> Canadian Association of Research Libraries, Commissioner of Canada's Proposals for ensuring appropriate regulation of artificial intelligence, March 2020, <u>https://www.carl-abrc.ca/wp-</u>

content/uploads/2020/03/CARL\_Submission\_Al\_and\_PIPEDA.pdf

<sup>&</sup>lt;sup>4</sup> Barclay, Donald A., PBS News, "Column: Can librarians help solve the fake news problem?" January 2017, https://www.pbs.org/newshour/education/column-can-librarians-help-solve-the-fake-news-problem

<sup>&</sup>lt;sup>5</sup> Joan Donovan, Claire Wardle and Kate Starbird, NBC News, "These disinformation researchers saw the coronavirus 'infodemic' coming", May 2020 https://www.nbcnews.com/tech/social-media/these-disinformation-researchers-sawcoronavirus-infodemic-coming-n1206911

<sup>&</sup>lt;sup>6</sup> Ryan Holmes, Forbes, "How Libraries Are Reinventing Themselves To Fight Fake News", April 2018, https://www.forbes.com/sites/ryanholmes/2018/04/10/how-libraries-are-reinventing-themselves-to-fight-fakenews/?sh=49a80d8afd16

and our position as trusted community leaders. This is further supported in a recent article in The Guardian where Joan Donovan, a misinformation scholar at Harvard, noted that "10,000 librarians"<sup>8</sup> are needed to address the misinformation crisis.

Declining trust in the government and the mainstream media<sup>9</sup> have created a fertile environment for misinformation to spread. Much of this misinformation can be credited to far-right publications with billionaire backers, like The Epoch Times, or viral online cults like QAnon, but the problem is even more widespread. Misinformation also fills a social gap. Former QAnon adherent Lenka Perron told the New York Times<sup>10</sup> about how, feeling abandoned by politicians and ignored by the media, she found emotional support among Q believers. The fact that so many are only able to find community among conspiracy theorists, whose narratives are frequently racist and anti-Semitic, raises serious concerns. Stories like Perron's demonstrate that the response to misinformation can't only be teaching people how to evaluate the news.

Misinformation researchers<sup>11</sup> and librarians<sup>12</sup> identify the rise of "Big Tech" whose algorithms promote the most incendiary voices as a major driver of misinformation online. Big Tech dominates the information landscape with billions of users, creates vectors of "fake news," and undermines librarians' ability to serve as information stewards. Librarians are simply not equipped to combat these issues when advertising and social media giants like Facebook and YouTube design their algorithms to encourage maximum engagement<sup>13</sup> rather than accuracy or reliability. While platforms like Twitter are finally attempting to combat misinformation, corporations should not be allowed to serve as the sole arbiters of speech in a democracy.

One crucial tool for combating misinformation is to increase funding for Canada's libraries. All schools need a librarian. Universities and colleges need funding for

<sup>12</sup> Amy Carlton, American Libraries Magazine, "Libraries and Invasive Technology", January 2021 https://americanlibrariesmagazine.org/blogs/the-scoop/libraries-and-invasive-technology/

<sup>&</sup>lt;sup>7</sup>Nicole Higgins DeSmet, USA Today, "School librarians teach CRAAP to fight fake news", July 2017, https://www.usatoday.com/story/news/nation-now/2017/07/25/school-librarians-teach-craap-fight-fakenews/507105001/

<sup>&</sup>lt;sup>8</sup> Julia Carrie Wong, The Guardian, "Banning Trump won't fix social media: 10 ideas to rebuild our broken internet – by experts", January 2021 https://www.theguardian.com/media/2021/jan/16/how-to-fix-social-media-trump-ban-free-speech

<sup>&</sup>lt;sup>9</sup> Christy Somos, CTV News, "Only 53 per cent of Canadians trust core institutions, report says", January 2020, https://www.ctvnews.ca/canada/only-53-per-cent-of-canadians-trust-core-institutions-report-says-1.4775238 <sup>10</sup> Sabrina Tavernese, The New York Times, "Trump Just Used Us and Our Fear': One Woman's Journey Out of QAnon", January 2021, https://www.nytimes.com/2021/01/29/us/leaving-ganon-conspiracy.html

<sup>&</sup>quot; Supra note 2, https://www.nbcnews.com/tech/social-media/these-disinformation-researchers-saw-coronavirusinfodemic-coming-n1206911

<sup>13</sup> Joan Donovan and Ahmed Khan, The Guardian, " Big tech was allowed to spread misinformation unchecked. Will Biden hold them accountable?" January 2021,

https://www.theguardian.com/technology/commentisfree/2021/jan/27/ganon-facebook-google-twittermisinformation-big-tech

library staffing to help improve information literacy and to invest in resources and infrastructure that accelerates the shift towards Open Science and Open Access publishing, improving access to reputable and verifiable information online. Municipalities must invest in the things that help build communities -- housing, parks, schools, recreation facilities, and, of course, libraries. Libraries are also the only source of internet access for many Canadian citizens. In a 2011 report from OCLC, researchers found that Canadian public libraries supported 3.2 million free wi-fi connections annually with internet use through library workstations surpassing 18 million. Access to the internet was declared a human right by the United Nations in 2016. With this in mind, the Canadian government should make universal broadband an expedited priority, and fund library internet access.

Librarians are ready to bring our skills and values to this fight. We just need adequate and maintained funding in order to ensure that we have the resources to do so.<sup>14</sup>

#### 2. Curtail monopolistic social media platforms

As noted above, the Big Tech social media platforms like those identified in the discussion paper (e.g. Facebook, Instagram, Twitter, YouTube, TikTok, Pornhub) are designed for maximum engagement, promoting the most inflammatory opinions and voices and creating vectors of fake news. The impact of these design choices is compounded by the monopolistic tendencies of these companies, giving them unprecedented control over the content that Canadians access on the Internet. In a recent blog post, Cory Doctorow uses the example of Facebook, in that the company has grown exponentially in size through "a history of anticompetitive mergers -Whatsapp, Instagram, Onavo and more - based on fraudulent promises to antitrust regulators". Doctorow notes that through this practice, "FB set out to acquire a monopoly and extract monopoly rents from advertisers and publishers, with a pathological indifference to how these frauds would harm others".<sup>15</sup> He goes on to demonstrate, using the example of Facebook's legal challenges to Adobserver, that the company is actively hostile towards organizations that try and ensure that they are accountable in their promises to limit misinformation through labelling political ads and blocking paid disinformation.<sup>16</sup>

In order to effectively combat online harm, Canada must closely examine the anticompetitive and monopolistic practices of these Big Tech companies. Big Tech must be held accountable and must face actual consequences for the harm that they inflict.

https://pluralistic.net/2021/09/22/kropotkin-graeber/#zuckerveganism

<sup>&</sup>lt;sup>14</sup> This section was adapted, with permission, from an unpublished article on misinformation and libraries drafted by members of the Library Freedom Project.

<sup>&</sup>lt;sup>15</sup> Doctorow, Cory. Facebook algorithm boosts pro-Facebook news. 22 Sept. 2021.

<sup>&</sup>lt;sup>16</sup> Doctorow, Corpy. Facebook escalates war on accountability. 5 Aug 2021.

## Commentary on the Discussion Guide and the Technical Paper

## 3. Penalties for non-compliance

Our comments on the monopolistic tendencies in Big Tech directly relate to the significant penalties for non-compliance that have been outlined in the Discussion Paper. As with the GDPR, deep pockets and vast resources are required to comply with the complicated and onerous requirements in the proposed online harm legislation. Research libraries appreciate that the online services that we offer appear to fall outside of the proposed legislation, but we also feel that it is important to ensure that organizations that represent the public interest like Wikipedia, the Internet Archive, Project Gutenberg and others are also exempted. These organizations would likely not have the resources to comply, are not actively promoting online harm, and include much content that can be used to combat the spread of misinformation. Forcing them to comply with these requirements may actually force them to stop operations in Canada, further cementing the dominance and control that big tech has over the contents on the internet. As noted by Doctorow, new internet regulations like the General Data Protection Regulation (GDPR) have "done more to enshrine Big Tech's dominance than the decades of lax antitrust enforcement that preceded them. This will have grave consequences for privacy, free expression and safety."17

#### 4. Guarding against the over-removal of content

CARL is concerned that the proposed approach may result in the significant overremoval of content. Without any measures to compel platforms to mitigate such overreach, this loss of content will harm the public historical record as well as small, independent content producers that depend on these platforms.

In comments that we submitted to the government that relate to the right to be forgotten (RTBF), we note that, any such right must:

- Aim to balance an individual's right to privacy with others' freedom of expression.
- Protect from the over-removal of content.
- Respect the integrity of the historical record.<sup>18</sup>

<sup>&</sup>lt;sup>17</sup> Doctorow, Cory. Regulating Big Tech makes them stronger, so they need competition instead. The Economist. Jun 6, 2019. <a href="https://www.economist.com/open-future/2019/06/06/regulating-big-tech-makes-them-stronger-so-they-need-competition-instead">https://www.economist.com/open-future/2019/06/06/regulating-big-tech-makes-them-stronger-so-they-need-competition-instead</a>

<sup>&</sup>lt;sup>18</sup> CARL response to Modernizing Privacy in Ontario Empowering Ontarians and Enabling the Digital Economy. https://www.carl-abrc.ca/wp-content/uploads/2021/09/2021\_CARL\_Response\_Mondernization\_Privacy\_Ontario.pdf

These three principles are also very relevant in this context. Over-removal in a RTBF regime or in an online harm regime as described will impact individual freedom of expression rights, increase the spectre of censorship and damage the historical record. This final point is of paramount importance to libraries. Information on the Internet may have future value for both the public and for researchers and we believe that an expert assessment of the impact of the removal on the historical record should form part of every decision to remove information from the internet.

Canadian libraries are also concerned that the proposal requires the use of algorithmic filters and AI driven tools to facilitate the removal of content. These problems are exacerbated by the 24-hour removal timelines and massive penalties for companies that fail to remove banned content. This will all-but guarantee that the system will lead to the mass removal of content. In addition, with no penalties in place for companies that over-remove content, there will be no incentive to restore content that was removed erroneously.

As noted in the commentary by Matt Hatfield from Open Media,

The more our government leans on platforms to remove content quickly through this legislation, the more they'll have to rely on algorithms that will flag for removal satire and humour, documentation of human rights abuses and attacks, sex education and voluntary sexual expression, conversation within marginalized communities about their experience, and more— not just the intended targeted hateful or violent content. Even if a human reviewer needs to approve the algorithm's suggestion, the legal incentives and limited time they have to make a decision will encourage removing all but the most obviously innocuous types of flagged content.<sup>19</sup>

Canadian libraries have tangible examples of how algorithmically driven removal tools controlled by private companies can impact the public record. For example, the University of Calgary Copyright Office discovered that Leni Riefenstahl's 1935 documentary "Triumph of the Will", was removed from YouTube shortly following the announcement of its new standards, claiming it fell under the category of "videos that promote or glorify Nazi ideology, which is inherently discriminatory,...".<sup>20</sup> This film is used in many history classes across the country to study nazi Germany, and is an important historical artifact.

The use of AI for monitoring and removing online content goes against the very premise of net neutrality, something that the Canadian government formally

<sup>20</sup> YouTube Pulls 'Triumph of the Will' for Violating Hate Speech Policy

<sup>&</sup>lt;sup>19</sup> A First Look at Canada's Harmful Content proposal. <u>https://openmedia.org/article/item/a-first-look-at-canadas-</u> harmful-content-proposal

https://www.indiewire.com/2019/06/youtube-hate-speech-policy-triumph-of-the-will-1202147879/

recognized in a motion in parliament in 2018.<sup>21</sup> Further supporting the government's adoption in Parliament, the Canadian Telecommunications Act - S.C. 1993, c. 38, specifically has safeguards embedded within legislation against discrimination and content control:

- Canadian Telecommunications Policy, 7 (a) to facilitate the orderly development throughout Canada of a telecommunications system that serves to safeguard, enrich and strengthen the social and economic fabric of Canada and its regions;<sup>22</sup>
- Section 36 Except where the Commission approves otherwise, a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public.<sup>23</sup>

By implementing a system that is charged with broad, sweeping reviews of high level content with the intention of removal goes against current Canadian legislation, the principle of net neutrality, and has the potential to jeopardize intellectual freedom, "especially those who may have specific needs or come from groups which are marginalized or subject to discrimination".<sup>24</sup>

#### 5. Expected Effects on Marginalized Communities

The increasing use of AI to identify and remove content brings with it a myriad of concerns related to privacy, some of which are human rights (by reinforcing bias and systemic racism) and transparency in decision making.<sup>25</sup> Increasingly, discussions related to the ethical use of AI technology and algorithms come into play, but the more complex the algorithm, the more opaque the decision making process becomes and inherently leads to greater racial biases.<sup>26</sup> These biases have significant implications for marginalized communities.

Examples of this type of bias can be seen in methods such as "predictive policing technologies that use historical and real time data to predict when and where a crime is most likely to occur or who is most likely to engage in or become a victim of criminal activity."<sup>27</sup> This is further demonstrated in findings by researchers at

https://www.ourcommons.ca/members/en/john-oliver(88881)/motions/9630989

https://www.ohchr.org/Documents/Issues/Opinion/ContentRegulation/IFLA.docx

<sup>25</sup> Modernizing Canada's Privacy Act, Brief by the Canadian Association of Research Libraries (2021),

<sup>&</sup>lt;sup>21</sup> M-168 Net Neutrality, 42nd Parliament, 1st Sessions, Decision: Agreed To (May 2018),

 <sup>&</sup>lt;sup>22</sup> Telecommunications Act S.C. 1993, c. 38, <a href="https://laws-lois.justice.gc.ca/eng/acts/t-3.4/page-1.html#h-459827">https://laws-lois.justice.gc.ca/eng/acts/t-3.4/page-1.html#h-459827</a>
 <sup>23</sup> Ibid

<sup>&</sup>lt;sup>24</sup> Comments by the International Federation Of Library Associations And Institutions (IFLA) to the Content Regulation in the Digital Age 2018 Human Rights Council Report

https://www.carl-abrc.ca/wp-content/uploads/2021/02/210212\_CARL\_Brief\_Modernizing\_Canada\_Privacy\_Act.pdf <sup>26</sup> Richardson, Rashida and Schultz, Jason and Crawford, Kate, Dirty Data, Bad Predictions: How Civil Rights

Violations Impact Police Data, Predictive Policing Systems, and Justice (February 13, 2019), 94 N.Y.U. L. REV. ONLINE 192 (2019), Available at SSRN: https://ssrn.com/abstract=3333423

<sup>&</sup>lt;sup>27</sup> Nani Jansen Reventlow, How Artificial Intelligence Impacts Marginalised Groups, Digital Freedom Fund, May 2021, https://digitalfreedomfund.org/how-artificial-intelligence-impacts-marginalised-groups/

Stanford University and McMaster University using GPT-3, an AI system that generates text. The researchers explored the capabilities of the algorithms to generate jokes based on partial sentences entered for analysis. It resulted with the use of the word "Muslim" persistently resulting in generating violent text.<sup>28</sup> These examples display the potential for algorithms to predict potential harms deriving from biased algorithms that could not only remove content by, and about, marginalized communities from the internet unnecessarily, but also provide unwarranted and erroneous information about specific communities to policing agencies.

Another flaw in this system is that individuals and groups that promote racism and hate speech can use the reporting systems on these platforms to silence marginalized communities. Creating a legal framework that imposes quick turnaround times for the removal of content and leaves the responsibility for compliance to the online communication service provider (OCSP) will result in accounts being blocked and posts being removed. This enables bad actors to attack views that they oppose, thereby causing a more harmful experience for marginalized communities as opposed to providing a safe space for sharing viewpoints and discussion.

## Potential impact of new regulators and dependance on law enforcement

The government proposal would create an administratively burdensome process overseen by a powerful new regulatory body that effectively has the authority to broadly interpret what qualifies as harmful content and determine sanctions, including significant financial penalties, based on its analysis.

As noted by Michael Geist:

"The new commissioner would be empowered to hold hearings on any issue, including non-compliance or anything that the Commissioner believes is in the public interest. The Digital Safety Commissioner would have broad powers to order the OCSs "to do any act or thing, or refrain from doing anything necessary to ensure compliance with any obligations imposed on the OCSP by or under the Act within the time specified in the order."<sup>29</sup>

While the Digital Recourse Council of Canada will provide Canadians with a last chance review of their case, the likelihood of delays and a long-drawn-out review

 <sup>&</sup>lt;sup>28</sup> Abubakar Abid, Maheen Farooqi and James Zou, "Large language models associate Muslims with violence", Nature Machine Intelligence | VOL 3 | June 2021 | 461-463 | https://doi.org/10.1038/s42256-021-00359-2
 <sup>29</sup>Picking Up Where Bill C-10 Left Off: The Canadian Government's Non-Consultation on Online Harms Legislation, https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/

process followed by binding decisions could result in content and OCS's being in limbo for years.

The proposed approach also includes mandatory reporting requirements to law enforcement and record retention by OCSPs but lacks provisions that would ensure users' privacy rights. Furthermore, the Digital Safety Commissioner would be granted overarching inspection powers of OCSPs and related companies, the ability to order website blocking and impose other obligations and penalties on OCSPs, with hearings potentially held in secret.

Reporting requirements to the RCMP and CSIS raise particular concerns. Protecting children and vulnerable and marginalized communities from online harm is a priority, however, the resulting regulation must include clear transparent protocols that prevent a surveillance state and mis-categorization of individuals. As Open Media has noted, "this proposal will create an unprecedented system of online surveillance of ordinary people in Canada and normalize the removal of much entirely lawful online speech. It won't make online spaces safer or more pleasant, and it is likely to hurt folk with marginalized identities the most."<sup>30</sup>

To complicate these issues even further, platforms will be required to report content they remove directly to law enforcement, including the RCMP and CSIS. Under this regime, users will not be made aware they have been reported, and there is nothing identified in this consultation that would regulate how that information is used by law enforcement with the information received. With the proposed methods in managing information and the serious problems raised earlier in this brief with regards to overremoval of content, biases in automated decision making, and the requirement for immediate removal of content without measured judgement, this leaves Canadians exposed to unnecessary and unwarranted policing with little or no recourse by individuals.

# Conclusion

Canadian research libraries agree that Canadian citizens deserve a "safe, inclusive, and open online environment" but the proposed approach to regulating social media and combating harmful content online needs a great deal of critical thinking and caution. CARL is available to discuss the issues and recommendations detailed above.

CARL is the voice of Canada's research libraries. Our members include Canada's twenty-nine largest university libraries and two federal institutions. CARL enhances

<sup>&</sup>lt;sup>30</sup> A First Look at Canada's Harmful Content Proposal, <u>https://openmedia.org/article/item/a-first-look-at-canadas-</u> harmful-content-proposal

its members' capacity to advance research and higher education; promotes effective and sustainable knowledge creation, dissemination, and preservation; and advocates for public policy that enables broad access to scholarly information. CARL's two federal member institutions contribute to Canada's research enterprise and collaborate in coordinated efforts with the academic library community, but do not engage in CARL's federal advocacy.

Mod Rocki, a solida Spin, a constituina a los as Processos and a relations May operate a transmission a spin V 20 Stantinetti a transmission V



September 24, 2021

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St. Gatineau QC K1A 0S5 pch.icn-dci.pch@canada.ca

#### Re: "The Government's proposed approach to address harmful content online"

Please find attached CBC/Radio-Canada's written submission with respect to "the Government's proposed approach to make social media platforms and other online communications services more accountable and more transparent when it comes to combating harmful content online," as released on July 29, 2021.

With a focus on online threats to journalists and those who work for news media organizations – and, by extension, threats to freedom of expression, diversity of voices, and the underpinnings of our democracy – our comments primarily relate to two (2) of the five (5) categories of harmful content: Content that incites violence; and hate speech.

In addition to providing background and additional context, this submission also includes five (5) specific recommendations.

CBC/Radio-Canada understands that the Government will be holding roundtable discussions and focused conversations on this topic in the near future, and would be pleased to participate in that phase of the process as well.

Sincerely,

Claude Galipeau Executive Vice-President, Corporate Development, CBC/Radio-Canada

# TABLE OF CONTENTS

Executive Summary	3
Introduction	5
Allocating responsibilities: Addressing the threat to journalists	7
International Benchmarking (especially the United Kingdom)	9
Specific recommendations with respect to the Discussion Guide and Technical Paper	11
Recommendation No. 1	11
Recommendation No. 2	12
Recommendation No. 3	13
Recommendation No. 4	14
Recommendation No. 5	15
Appendix	18
Section 14 of the United Kingdom's Draft Online Safety Bill	

2

#### **Executive Summary**

CBC/Radio-Canada applauds the Department's commitment to develop and implement an approach to make social media platforms and other online communications services more accountable and transparent with respect to harmful content online.

However, we believe an important issue has been overlooked in this process – one that not only risks individual safety (which can never be tolerated), but also challenges the very foundations of freedom of expression, diversity of voices, and the underpinnings of democracy itself; namely, online threats against journalists and others who work for news media organizations (collectively, journalists).

Detailed studies by organizations such as UNESCO and Reporters Sans Frontières have confirmed that threats born in an online environment migrate to the physical world; and women and racialized journalists are particularly targeted and vulnerable. News organizations, including CBC/Radio-Canada, have a moral obligation to ensure that journalists are free to seek out and report on stories without the fear of physical or psychological retribution.

In this process, and in eventual legislation, we believe that the Government should clearly express that such threats are unacceptable and will not be tolerated – and this message must be established in the strongest possible ways: With strong enforcement mechanisms, mandatory monitoring and reporting, transparent and well-publicized policies, and swift complaint assessment and appeals processes.

CBC/Radio-Canada makes the following five (5) recommendations:

- 1. Include explicit recognition of online threats to journalists directly into the Act, and afford "exceptional recourse" to these types of threats.
  - CBC/Radio-Canada is not recommending the addition of a new category of harmful content in the legislation. Rather, we are seeking to maintain the proposed five (5) categories of harmful content, but include explicit recognition of online threats to journalists due to the special and corrosive damage such threats can cause – not just to individuals, but also to freedom of expression, diversity of voices, and civil and safe discourse.
- The Advisory Board should always include at least one practising journalist who has direct and recent experience in print, broadcasting, or digital journalism. The Governor in Council should consult with relevant news associations or bodies prior to appointing this individual to the Advisory Board.
  - The Digital Safety Commission and Recourse Council should always have a ready
    resource available to understand the sensitivities and concerns of journalists in the field
     including journalists from equity-seeking groups who can be even more at risk from
    social media posts and calls to action.

3

- The legislation should explicitly recognize that "doxing" (or "doxxing") is a form of incitement to violence.
  - The online release of personal details, including location information, can lead to devastating attacks. CBC/Radio-Canada submits that the purposeful public release of such information online should be considered evidence of online harm prima facie by social media platforms, the Recourse Council, and the Digital Safety Commissioner, and particularly under the category of content that incites violence.
- 4. The proposed number of decision-makers on the Recourse Council is insufficient to achieve the Government's objectives as they relate to diversity and subject matter experts. We recommend a larger pool of decision-makers that could draw upon the membership of the Advisory Council.
  - Members of the Advisory Board as that body is described in paragraphs 71-75 of the Technical Paper could perhaps serve in this role. The Chair of the Recourse Council, in consultation with the Chairperson of the Advisory Board, could effectively deputize a member(s) of the Advisory Board to participate in a complaint proceeding and directly contribute to its resolution. This would effectively broaden and diversify the decision-making process by making the pool larger, add the most appropriate subject matter experts directly into decision-making, and prevent needless delays based on the availability of Recourse Council members or other scheduling concerns.
- 5. Given the potentially damaging and destructive nature of harmful online materials, we urge the Government to set firm timelines in the legislation for *all* of the various steps.
  - Every minute that harmful material is publicly available on social media magnifies the risk to individuals and property. While the draft legislation contemplates a 24-hour period for social media platforms to consider content that has been flagged, it has not set firm timelines for platform reconsideration or Recourse Council processes, including final determination.

We also believe that the Government should continue to benchmark its efforts against international standards and legislation (or draft legislation), particularly recent activities in the United Kingdom and Australia.

#### Introduction

 In 2020, UNESCO released a report on the impact of online harassment and abuse toward journalists, and particularly female journalists.<sup>1</sup> The introduction of the report summarized the concerns as follows:

Online violence has since become a new frontline in journalism safety – a particularly dangerous trend for women journalists. The psychological, physical, and digital safety and security impacts associated with this escalating freedom of expression crisis are overlapping, converging and frequently inseparable. The phenomenon can be defined as a combination of: often brutal, prolific online harassment and abuse, including targeted attacks that frequently involve threats of physical and/or sexual violence; digital privacy and security breaches that can expose identifying information and exacerbate offline safety threats facing women journalists and their sources; and coordinated disinformation campaigns leveraging misogyny and other forms of hate speech. The perpetrators range from misogynistic mobs seeking to silence women, through to State-linked disinformation networks aiming to undercut press freedom and chill critical journalism via orchestrated attacks.

- 2. The UNESCO report included 31 key findings, many involving threats to personal safety. All of it is disturbing; and none of it is acceptable. Key Finding No. 1 was this: 73% of women respondents said they had experienced online violence in connection with their work in journalism. As a country, we would never allow such behaviour in the offline world. And yet 20% of women journalists in the same survey "reported experiencing abuse and attacks in the physical world that they believed were associated with online attacks."
- 3. Threats born in an online environment migrate to the physical world, and women and racialized journalists are particularly targeted and vulnerable. In fact, a survey conducted by Reporters Sans Frontières (RSF) in Summer 2020 concluded that "the internet has even become more dangerous for journalists than 'the street': it is now online that the most gender-based violence occurs."<sup>2</sup> A separate article highlights the real world peril that flows from online violence:

Our survey provides disturbing new evidence that online violence against women journalists is jumping offline. Frequently associated with <u>orchestrated attacks</u> designed to chill critical journalism, it migrates into the physical world – sometimes with deadly impacts.

In 2017, the Committee to Protect Journalists reported that in <u>at least 40% of cases</u>, journalists who were murdered had received threats, including online, before they were killed. The same year, two women journalists on opposite sides of the world were murdered for their work within six weeks of one another: celebrated Maltese investigative journalist <u>Daphne Caruana Galizia</u> and prominent Indian journalist <u>Gauri</u>

5

<sup>&</sup>lt;sup>1</sup> Julie Posetti et al., "Online violence against women journalists: a global snapshot of incidence and impacts," UNESCO, Catalog No. 0000375136, 2020, available at <u>UNESCO Report.</u>

<sup>&</sup>lt;sup>2</sup> Reporters Sans Frontières, "Journalism in face of sexism," March 8, 2021, p. 9, available via <u>Journée Internationale</u> des droits des femmes : RSF publie son enquête "Le journalisme face au sexisme" | RSF.

Lankesh. Both had been the targets of prolific, gendered online attacks before they were killed.<sup>3</sup>

4. News organizations, including CBC/Radio-Canada, have a moral obligation to ensure that journalists are free to seek out and report on stories without the fear of physical or psychological retribution. To do otherwise not only risks individual safety (which can never be tolerated), but also challenges the very foundations of freedom of expression, diversity of voices, and the underpinnings of democracy itself. Earlier this year, the European Broadcasting Union (EBU) described this wider impact as follows:

In addition to the psychological and professional harm, online violence against women journalists and media professionals can lead to self-censorship. Some women journalists and media professionals decide to use pseudonyms, others chose to suspend, deactivate or delete permanently their online accounts. Others even make the decision to leave their profession. Online violence targeting women journalists and media professionals deprive them from their fundamental rights, including the right to live free from violence, the right to freedom of expression and the right to privacy. Due to online violence and its consequences, the online information space and pluralism of the media are seriously damaged.<sup>4</sup>

5. UNESCO also emphasized the chilling effect of online threats to journalists:

Many women journalists self-censor in response to online violence. Nearly a third (30%) of our survey respondents said they self-censor on social media as a result of being targeted, while 20% said they avoid all interaction online, and 18% said they specifically avoided engaging with audiences. Such acts could be considered defensive measures designed to preserve their safety, but they also demonstrate the effectiveness of online attack tactics – designed to chill critical reporting, silence women, and muzzle truth-telling.<sup>5</sup>

6. As a country, we cannot just accept this type of online harm. The intimidation of journalists and other media professionals has increased in volume and ferocity during the pandemic, and it must stop.<sup>6</sup> We cannot risk their personal safety; and we cannot allow critical reporting to go unpublished or stories to remain hidden. We cannot allow certain actors to chase news-gatherers and reporters – of any gender, of any background – out of the profession and

<sup>&</sup>lt;sup>3</sup> Julie Posetti, Jackie Harrison, and Silvio Waisbord, "Online attacks on female journalists are increasingly spilling into the 'real world' - new research," *The Conversation*, November 25, 2020.

<sup>&</sup>lt;sup>4</sup> EBU, "EBU Contribution to the European Commission's Consultation on Gender-Based Violence Against Women – Focus on Online Violence," May 10, 2021, available at <u>EBU Policy Position on Gender-Based Violence Against</u> <u>Women</u>. The EBU specifically cites a study presented by the Human Rights Council of the United Nations General Assembly entitled "Combatting violence against women journalists: Report of the Special Rapporteur on violence against women, its causes and consequences," May 6, 2020, available at <u>Human Rights Council of the United</u> <u>Nations Study</u>.

<sup>&</sup>lt;sup>5</sup> UNESCO, Key Finding No. 28, p. 13.

<sup>&</sup>lt;sup>6</sup> A report stemming from an online questionnaire prepared by the National Union of Journalists (NUJ) in Fall 2020 lists specific threats made against journalists in the United Kingdom. We recommend that the Government review this <u>survey</u> as it prepares its legislation.

allow that vacuum to be filled with unsubstantiated news, misinformation, disinformation, and fake news.

- 7. As outlined in this submission, other countries, such as the United Kingdom, are already taking tangible steps to address online threats to journalists.
- 8. This consultation process offers the potential for real, lasting change. CBC/Radio-Canada understands that crafting legislation in this area is a difficult exercise; but we are heartened that the "Government of Canada is committed to taking meaningful action to combat hate speech and other kinds of harmful content online."<sup>7</sup>
- 9. While many parties have a role to play (see below), there is no question that online communications service providers (OCSP) or, more colloquially, social media platforms are central to a solution, and must be more responsive and transparent when it comes to combating harmful content online.<sup>8</sup> They must be more consistent in applying internal policies and identifying and removing harmful content; and they must expedite decision-making and reconsiderations.
- 10. Moreover, if social media platforms are enabling this behaviour and attendant threats (and they are), then it is incumbent on the Government to address the issue head-on through the development of new and tougher legislation, enforcement, and, if necessary, financial penalties.

#### Allocating responsibilities: Addressing the threat to journalists

- 11. There is a role here for everyone.
- 12. News organizations need to provide appropriate training, security, and tools for their journalists and support staff in the field (including the monitoring of social media). They need to work with the various social media companies to identify and flag online content that incites violence and hate speech; and they need to work with the police and government authorities to make sure these threats are understood for what they are: Real threats to individual safety, freedom of expression, diversity of voices, and ultimately, the civil underpinnings of our open democratic society.
- 13. At CBC/Radio-Canada, 57% of our journalists are women.<sup>9</sup> They bring fresh angles to the stories we cover, and bring much needed gender parity to our reporting of current events. This year, we established a Task Force to Fight Online Hate that includes representatives from the CBC and Radio-Canada news teams, Legal, Corporate, and several members of the Senior Executive Team,

7

<sup>&</sup>lt;sup>7</sup> Department of Canadian Heritage, "Have your say: The Government's proposed approach to address harmful content online," July 29, 2021.

<sup>&</sup>lt;sup>8</sup> In this submission, we have used the terms "OCSP" and "social media platform" interchangeably. We recognize, however, that Module 1 of the Discussion Guide makes a distinction between the terms: "The concept of online communication service provider is intended to capture major platforms, (e.g., Facebook, Instagram, Twitter, YouTube, TikTok, Pornhub), and exclude products and services that would not qualify as online communication services, such as fitness applications or travel review websites."

<sup>&</sup>lt;sup>9</sup> See Catherine Tait, "Défendre les femmes jounalistes contre la haine en ligne," La Presse, April 20, 2021.

including the Chief Executive Officer. Presently, the Task Force is working on actions to actively discourage attacks and help our journalists when incidents occur. We are also benchmarking the plans and initiatives of other public broadcasters and media organizations around the world to see how we can improve our own operations. Amongst other things, this work can supplement the security measures we have put in place to protect the physical security of journalists in Canada and abroad.

- 14. Social media platforms need to establish and consistently apply policies for monitoring and reviewing online content (including through algorithms and artificial intelligence),<sup>10</sup> assess the content against their own internal policies and various domestic laws, swiftly remove content that violates those rules, and determine what future corporate actions might be taken against individuals or groups responsible for online threats against journalists and media professionals.<sup>11</sup>
- 15. In consultation with news organizations, journalists, and relevant associations, social media platforms should develop, publish, implement, and strictly adhere to streamlined processes to respond to, and otherwise address, online threats against journalists and media professionals. Open and direct lines of communications between all parties should be established, nurtured, and maintained to ensure that internal policies and procedures are regularly reviewed and that timelines are consistently met.
- 16. CBC/Radio-Canada understands that individuals may disagree on the acceptability or legality of a given piece of content; so, social media platforms must have a clear and transparent complaints-handling process one that recognizes that time is of the essence. As noted elsewhere in this submission, every minute that harmful material is publicly available on social media magnifies the risk to individuals and property.
- 17. The Government needs to clearly express that threats against journalists and media professionals are unacceptable and will not be tolerated and that social media platforms must play an active role in identifying, and acting upon, content that incites violence and hate speech. This message must be established in the strongest possible ways: Through legislation with strong enforcement mechanisms, mandatory monitoring and reporting, transparent and well-publicized policies, and swift complaint assessment and appeals processes.
- The Government should also continue to benchmark its efforts against international standards and legislation (or draft legislation), particularly recent activities in the United Kingdom and Australia.

8

<sup>&</sup>lt;sup>10</sup> According to the aforementioned survey by the National Union of Journalists in the United Kingdom: 93% of respondents said social media platforms do not robustly implement their own policies intended to deter and stop abuse; and 88% of respondents said that social media platforms should do more to combat abuse and harassment. <sup>11</sup> The Government has identified the overall problem in the Background section of the Discussion Guide: "Social media platforms have significant impacts on expression, democratic participation, national security, and public safety. These platforms have tools to moderate harmful content. Mainstream social media platforms have voluntary content moderation systems that flag and test content against their community guidelines. But some platforms take decisive action in a largely ad-hoc fashion. These responses by social media companies tend to be reactive in nature and may not appropriately balance the wider public interest. Also, social media platforms are not required to preserve evidence of criminal content or notify law enforcement about criminal content, outside of mandatory reporting for child pornography offences. More proactive reporting could make it easier to hold perpetrators to account for harmful online activities."

# International Benchmarking (especially the United Kingdom)

19. In the Ministerial Foreword of the United Kingdom's "National Action Plan for the Protection of Journalists" released on March 9 this year, the Rt. Hon. John Whittingdale, Minister of State for Media and Data and the Department for Digital, Culture, Media & Sport and the Rt. Hon. Victoria Atkins, Minister for Safeguarding, Home Office wrote:

Journalism in the United Kingdom has a long and proud history. Since the days of John Wilkes, journalists have never shied away from holding the powerful to account – and in so doing, their work has shaped our society.

Underneath this lies a fundamental principle: that a journalist, whatever their persuasion, can do their job to the best of their ability, without fear or favour.

Unfortunately, too many journalists working in the UK today can no longer take that right for granted, and are facing both abuse and threats to their personal safety as well as encroachments on their freedom of expression.

A world where journalists are silenced by either fear or censorship is a much poorer one. This government, which was elected on a manifest commitment to defend the freedom of the press, will be robust in shielding them from both. This action plan will help guard them from threats to their safety, while our forthcoming online safety legislation will enshrine in law protections for journalistic content and free debate.<sup>12</sup>

20. The United Kingdom's national action plan is broad and far-reaching, extending to police and prosecutors, education, and regulations. And it explicitly recognizes the special concerns of journalists:

[O]nline abuse - which can range from obscene messages to death or rape threats – continues to be the most significant safety challenge facing journalists. This abuse, which is often aimed at women and BAME [Black, Asian, and Minority Ethnic] journalists, can leave a lasting and chilling impact. It drives talented individuals away from the profession, and piece by piece, it corrodes our democratic values.

The government has recognised the importance of addressing this issue and is already taking action. The forthcoming Online Safety Bill will require companies to tackle abuse on their services and take reasonable steps to protect users' safety online, while all users, including journalists, will be better able to report abuse, and should expect to receive appropriate support from the relevant platform if they do so.

This Plan confirms the following commitments:

 The government will make the UK the safest place in the world to be online, through the introduction of an Online Safety Bill, and

<sup>&</sup>lt;sup>12</sup> GOV.UK, National Action Plan for the Protection of Journalists.

 Facebook and Twitter will respond promptly to complaints of threats to journalists' safety

Furthermore, the government is also looking at the criminal law and if it can more effectively address online abuse. A Law Commission review, sponsored by DCMS, has found the law in need of updating to address a range of abusive behaviours online, including pile-on harassment, cyber flashing and the glorification of self-harm, and the Commission has therefore consulted on proposed reforms, suggesting potential new offences to tackle the harms arising from online abuse. Where necessary and appropriate, legislation will be introduced.<sup>13</sup>

- 21. As seen above, the Government in the United Kingdom has clearly recognized that social media companies play a key role in protecting the safety of journalists and has specifically called out Facebook and Twitter in the process.
- 22. The United Kingdom's *Draft Online Safety Bill* also includes a dedicated section on journalistic content. For ease of reference, we have excerpted that section in the Appendix.
- 23. Of course, the United Kingdom is not alone in developing legislation to address elements of online harm. Australia introduced its *Online Safety Bill 2021* earlier this year. For ease of reference, we have excerpted the Summary of the Bill immediately below:

Introduced with the Online Safety (Transitional Provisions and Consequential Amendments) Bill 2021, the bill: retains and replicates certain provisions in the *Enhancing Online Safety Act 2015*, including the non-consensual sharing of intimate images scheme; specifies basic online safety expectations; establishes an online content scheme for the removal of certain material; creates a complaints-based removal notice scheme for cyber-abuse being perpetrated against an Australian adult; broadens the cyber-bullying scheme to capture harms occurring on services other than social media; reduces the timeframe for service providers to respond to a removal notice from the eSafety Commissioner; brings providers of app distribution services and internet search engine services into the remit of the new online content scheme; and establishes a power for the eSafety Commissioner to request or require internet service providers to disable access to material depicting, promoting, inciting or instructing in abhorrent violent conduct for time-limited periods in crisis situations.<sup>14</sup>

13 Ibid, the Plan, part 4.

<sup>14</sup> Australia's Online Safety Bill 2021.

## Specific recommendations with respect to the Discussion Guide and Technical Paper

24. CBC/Radio-Canada has carefully reviewed the Discussion Guide and Technical Paper and makes the following five (5) recommendations:

#### Recommendation No. 1

Include explicit recognition of online threats to journalists directly into the Act, and afford "exceptional recourse" to these types of threats.

CBC-Radio-Canada is not recommending the addition of a new category of harmful content in the legislation. Rather, we are seeking to maintain the proposed five (5) categories of harmful content, but include explicit recognition of online threats to journalists due to the special and corrosive damage such threats can cause – not just to individuals, but also to freedom of expression, diversity of voices, and the underpinnings of civil and safe discourse.

25. In the Discussion Guide attached to this process, the Government stated:

The legislation would target five categories of harmful content:

- terrorist content;
- content that incites violence;
- hate speech;
- non-consensual sharing of intimate images; and
- child sexual exploitation content.

While all of the definitions would draw upon existing law, including current offences and definitions in the Criminal Code, they would be modified in order to tailor them to a regulatory – as opposed to criminal – context.

These categories were selected because they are the most egregious kinds of harmful content. The Government recognizes that there are other online harms that could also be examined and possibly addressed through future programming activities or legislative action.

- 26. For clarity, while our submission is focused on online threats to journalists, we are not suggesting that this should be a category of harmful content unto itself. Rather, we believe that online threats to journalists fit squarely into two (2) categories of harmful content that have already been identified in this consultation process: content that incites violence; and hate speech.
- 27. We do recommend, however, that the Act incorporate into the legislation the duty of social media platforms to protect journalists similar to the way the United Kingdom has incorporated.

28. Moreover, given that threats to journalists not only impact individual safety but also, by extension, threats to freedom of expression, diversity of voices, and the underpinnings of our open democracy, we believe that "Exceptional Recourse" should be afforded to these types of threats and would amend paragraph 120 of the Technical Paper as follows:

Exceptional Recourse:

With the authority to apply to the Federal Court for an order requiring relevant Telecommunications Service Providers, as defined in subsection 2(1) of the *Telecommunications Act*, to block access in whole or in part to an offending OCS in Canada, if:

- a. an OCSP repeatedly demonstrates persistent non-compliance with orders solely with respect to removing the following harmful content:
  - I. child sexual exploitation content, or
  - II. terrorist content, or
  - III. threats against journalists; and
- b. all enforcement measures have been exhausted.
- 29. Online harm, in all of its incarnations, is unacceptable; but the Government should be clear in this legislation that threats against journalists merit exceptional recourse, as reserved for the most egregious of harms.
- 30. As a country, we should leave no doubt: Such threats are unacceptable and identifying and addressing such threats must never be taken lightly, nor should these files be deprioritized or delayed by a social media platform, or by any other party in the regulatory chain.

#### **Recommendation No. 2**

The Advisory Board should always include at least one practising journalist who has direct and recent experience in print, broadcasting, or digital journalism. The Governor in Council should consult with relevant news associations or bodies prior to appointing this individual to the Advisory Board.

The Digital Safety Commission and Recourse Council should always have a ready resource available to understand the sensitivities and concerns of journalists in the field – including journalists from equity-seeking groups who can be even more at risk from social media posts and calls to action.

31. Paragraph 72 of the Technical Paper describes the expected composition of the Advisory Board as follows:

> The Act should provide that in appointing members, the Minister take into consideration the importance of having members that are knowledgeable about or have experience related to law, technology, equity and social science, and are drawn from advocacy groups, including civil liberties, equity or victim advocacy organizations, the online communication industry, and academia.

32. Paragraph 75 outlines the functions of the Advisory Board as follows:

The Act should provide that the functions of the Advisory Board are to support and advise the Digital Safety Commissioner and the Digital Recourse Council of Canada by reporting regularly, and publicly, on emerging industry trends and technologies and on content-moderation practices.

- 33. CBC/Radio-Canada submits that the Advisory Board should include at least one member who is knowledgeable about, or has experience related to, modern journalism practices and ethics. In the most basic terms, threats to journalists chill freedom of expression, risk the ability to hold those in positions of power accountable, and generally imperil the foundations of our open democracy. The Digital Safety Commissioner and Recourse Council should always have a ready resource available to understand the sensitivities and concerns of journalists in the field including journalists from equity-seeking communities who can be even more at risk from social media posts and calls to action.
- 34. To this end, we submit that the wording in paragraph 72 of the Technical Paper be changed to:

The Act should provide that in appointing members, the Minister take into consideration the importance of having members that are knowledgeable about or have experience related to law, <u>journalism</u>, technology, equity and social science, and are drawn from advocacy groups, including civil liberties, equity or victim advocacy organizations, the online communication industry, and academia.

35. We further submit that the Advisory Council must always include at least one practising journalist who has direct and recent experience in print, broadcasting, or digital journalism; and further that the Governor in Council consult with relevant news associations or bodies prior to appointing this individual to the Advisory Board.

#### **Recommendation No. 3**

#### The legislation should explicitly recognize that "doxing" (sometimes referred to as "doxxing") is a form of incitement to violence.

36. Last year, the Human Rights Council of the United Nations General Assembly issued a report entitled "Combatting violence against women journalists: Report of the Special Rapporteur on violence against women, its causes and consequences."<sup>15</sup> The following was included as paragraph 48:

> Perhaps one of the most chilling factors is that for a number of women journalists harassment does not always remain online and has often spilled over into reality. In November 2017, shortly after publishing a report criticizing Internet trolls for sabotaging an application (app) used by women to report instances of harassment in the street, a woman journalist was the target of cyberattacks herself. She received a flood of emails

<sup>&</sup>lt;sup>15</sup> Human Rights Council of the United Nations Study.

threatening her with rape and violence, and attempts were made to hack her social networks and accounts. The attacks escalated with "doxing" attacks, meaning that her personal details and home address were publicly leaked. Her home address was used to register her name on pornography and paedophile websites.

37. The online release of personal details, including location information, can lead to devastating attacks. CBC/Radio-Canada submits that the purposeful public release of such information online should be considered evidence of online harm *prima facie* by social media platforms, the Recourse Council, and the Digital Safety Commissioner, and particularly under the category of content that incites violence. Doxing, in other words, should be an immediate concern in content removal policies and considerations/reconsiderations, and in Recourse Council complaint review processes. When parties determine that doxing has indeed taken place, removal of that information online must be swift.

#### **Recommendation No. 4**

The proposed number of decision-makers on the Recourse Council is insufficient to achieve the Government's objectives as they relate to diversity and subject matter experts. We recommend a larger pool of decision-makers that could draw upon the membership of the Advisory Council.

38. Paragraph 46 of the Technical Paper reads as follows:

The Act should provide that the Digital Recourse Council of Canada will be composed of no fewer than three (3) and no more than five (5) members, appointed by the Governor in Council. The Governor in Council will designate one (1) member as the Chairperson and may designate one (1) member as the Vice-Chairperson. The Act should provide that in appointing members, the Governor in Council shall take into consideration the importance of diverse subject-matter experts reflective of the Canadian population, particularly inclusive of women, Indigenous Peoples, members of racialized communities and religious minorities, of LGBTQ2 and gender-diverse communities, and persons with disabilities.

- CBC/Radio-Canada supports the Government's position that the Recourse Council reflect an increasingly diverse Canadian population.
- 40. However, with a membership that could be as small as three (3) individuals, we submit that achieving diverse and appropriate reflection of the country will be difficult to achieve. Even recognizing that an individual may be intimately familiar with or represent more than one of the groups listed, we do not see how a council of this size could adequately reflect contemporary Canada.
- 41. Similarly, while the Government is seeking a composition of the Recourse Council that would include "diverse subject matter experts" we do not understand how that objective could be accomplished with a council membership capped at 3-5 members. This is especially relevant given the critical role the Recourse Council will play in reviewing key complaints. Per paragraph 45:

The Act should provide for the establishment of the Digital Recourse Council of Canada, whose functions are to:

- Receive and review complaints by affected persons in Canada stemming from content moderation decisions issued by OCSPs; and
- Issue decisions on such complaints regarding whether content qualifies as harmful content, as defined in legislation.
- 42. It is simply difficult to see how the Government would be able to establish and maintain a Recourse Council of this size and still achieve its objectives as they relate to diversity and subject matter experts. A larger Recourse Council could perhaps address this problem.
- 43. At the design stage of the regime, however, we suppose the Government may be concerned that there may not be enough complaints generated to warrant a larger council. If this is indeed the case, we recommend that the Government establish a full-time, dedicated Recourse Council and also a pool of diverse subject matter experts that could be drawn-upon to join the decision-making process.
- 44. Members of the Advisory Board as that body is described in paragraphs 71-75 of the Technical Paper – could perhaps serve in this role. The Chair of the Recourse Council, in consultation with the Chairperson of the Advisory Board, could effectively deputize a member(s) of the Advisory Board to participate in a complaint proceeding and directly contribute to its resolution. This would effectively broaden and diversify the decision-making process by making the pool larger, add the most appropriate subject matter experts directly into decision-making, and prevent needless delays based on the availability of Recourse Council members or other scheduling concerns. Moreover, as members of the Advisory Board would be appointed by the Governor in Council on a part-time basis, and paid for their involvement, they would already be familiar with the workings of the Recourse Council, relevant industry trends, and key precedent decisions. They would also be an inherently diverse group to draw upon since paragraph 71 of the Technical Paper mandates that the Advisory Board be reflective of the Canadian population.

#### **Recommendation No. 5**

Given the potentially damaging and destructive nature of harmful online materials – risks to personal safety; and threats to freedom of expression, diversity of voices, and the underpinnings of our open democracy – we urge the Government to set firm timelines in the legislation for <u>all</u> of the various steps.

While the draft legislation contemplates a 24-hour period for social media platforms to consider content that has been flagged, it has not set firm timelines for platform reconsideration or Recourse Council processes, including final determination.

45. Speed is a critical consideration: Every minute that harmful material is publicly available on social media magnifies the risk to individuals or property.

46. The Technical Document proposes a 24-hour timeframe for social media platforms to address content that has been flagged:

The Act should provide that an OCSP must address all content that is flagged by any person in Canada as harmful content, expeditiously after the content has been flagged.

- a. [B] The Act should provide that for part [A], "expeditiously" is to be defined as twenty-four (24) hours from the content being flagged, or such other period of time as may be prescribed by the Governor in Council through regulations.
- b. The Act should provide that in respect of part [A], "address" signifies that the OCSP must respond to the affected person stating that the content either a) does not meet the definition of harmful content, or b) does meet the definition of harmful content and has been made inaccessible to persons in Canada. In the latter situation, the OCSP must also make the content inaccessible in Canada within the timeframe required by part [B], and assess that content with respect to its obligations under parts [E] and [F].
- c. The Act should provide that in prescribing a new timeframe as provided for in part [B], the Governor in Council may prescribe through regulations different timelines for different types or subtypes of harmful content. The Act should provide that the new timeframes could be either extended or shortened from the timeframe provided in part [B].
- 47. This timeframe is consistent with content removal timelines included in Australia's Online Safety Bill 2021.<sup>16</sup> The Australian model also includes financial penalties for non-compliance with the timeline.
- 48. Per subsection (c) above regarding "different timelines for different types or subtypes of harmful content," we submit that the Governor in Council should always prescribe the shortest possible timelines for harmful content that affects journalists.
- 49. Our concerns on timing primarily relate to the reconsideration process at the social media platform, and, if necessary, subsequent review of a complaint by the Recourse Council after decisions have gone through the relevant content moderation and reconsideration processes at the platform level. There appear to be no firm timelines contemplated for these phases.
- 50. CBC/Radio-Canada understands that reconsideration and complaints processes can be difficult and that each party must have access to a fair and transparent process that may require the production of materials and the opportunity for debate and representation. But given the potentially damaging and destructive nature of harmful online materials (particularly when they are left online), and risks to personal safety and freedom of expression, we urge the Government to set firm timelines, or at least expected deadlines, in the legislation for all of the various steps.

<sup>&</sup>lt;sup>16</sup> Jason Scott and Vlad Savov, "Australian Law Could Force Facebook, Google to Strip Content," Bloomberg.com, June 22, 2021.

- 51. Given the stakes involved, social media platforms must not be afforded unlimited time, or even liberal time limits, in their reconsideration processes.
- 52. Furthermore, the Digital Safety Commissioner and Recourse Council should have strict timelines to complete the complaint review process and render a decision. As above, a small pool of decision-makers might appear more efficient; but it would clearly increase the risk of delay. In line with Recommendation No. 4 above, a bigger Recourse Council or larger pool of decision-makers could accelerate consideration of complaints and determinations.
- 53. Finally, paragraph 55 of the Technical Paper states: "The Act should ensure that the order contains a timeline for compliance." We believe that the timeline for compliance after a Recourse Council decision to remove harmful content is rendered should be set consistently in the *Act*, and should be no longer than 24 hours.

## Appendix

#### Section 14 of the United Kingdom's Draft Online Safety Bill

#### NOTES:

- The Draft Online Safety Bill was presented to Parliament by the Minister of State for Digital and Culture by Command of Her Majesty in May 2021
- Subsection 2(1) of the Draft Online Safety Bill defines "user-to-user service" as follows: "an
  internet service by means of which content that is generated by a user of the service, or
  uploaded to or shared on the service by a user of the service, may be encountered by another
  user, or other users, of the service."

#### 14 Duties to protect journalistic content: Category 1 services

- The "duties to protect journalistic content" in relation to user-to-user services are the duties set out in this section.
- A duty to operate a service using systems and processes designed to ensure that the importance
  of the free expression of journalistic content is taken into account when making decisions
  about
  - a. how to treat such content (especially decisions about whether to take it down or restrict users' access to it), and
  - b. whether to take action against a user generating, uploading or sharing such content.
- A duty, in relation to a decision by a provider to take down content or to restrict access to it, to
  make a dedicated and expedited complaints procedure available to a person who considers the
  content to be journalistic content and who is
  - a. the user who generated, uploaded or shared the content on the service, or
  - b. the creator of the content (see subsection (11)).
- 4. A duty to make a dedicated and expedited complaints procedure available to users of a service in relation to a decision by the provider of the service to take action against a user because of content generated, uploaded or shared by the user which the user considers to be journalistic content.
- 5. A duty to ensure that -
  - a. if a complaint about a decision mentioned in subsection (3) is upheld, the content is swiftly reinstated on the service;

- b. if a complaint about a decision mentioned in subsection (4) is upheld, the action against the user is swiftly reversed.
- 6. A duty to specify in the terms of service -
  - a. by what methods content present on the service is to be identified as journalistic content;
  - b. how the importance of the free expression of journalistic content is to be taken into account when making decisions mentioned in subsection (2);
  - c. the policies and processes for handling complaints in relation to content which is, or is considered to be, journalistic content.
  - 7. A duty to ensure that
    - a. the terms of service referred to in subsection (6) are clear and accessible, and
    - b. those terms of service are applied consistently.
- For the purposes of this section content is "journalistic content", in relation to a user-to-user service, if –
  - a. the content is -

i. news publisher content in relation to that service, or ii. regulated content in relation to that service;

- b. the content is generated for the purposes of journalism; and the content is UK-linked.
- 9. For the purposes of this section content is "UK-linked" if -
  - United Kingdom users of the service form one of the target markets for the content (or the only target market), or
  - b. the content is or is likely to be of interest to a significant number of United Kingdom users.
- 10. In this section references to "taking action" against a user are to giving a warning to a user, or suspending or banning a user from using a service, or in any way restricting a user's ability to use a service.
- 11. In this section the reference to a person who is the "creator" of content is a reference to any of the following
  - a. in the case of news publisher content, the recognised news publisher in question;
  - b. an individual who -

Description communities for in initial pri to (20) surfaceby d'information Majores d'internet description (2) the increase de Majormaliter (20)

i. created the content, and ii. is in the United Kingdom;

c. an entity which-

i. created the content, and

ii. is incorporated or formed under the law of any part of the United Kingdom.

12. For the meaning of "news publisher content", "regulated content" and "recognised news publisher", see sections 39 and 40.

Stocknester, and a stock of the access of the access of the stock o



September 25, 2021

# Submission of BSA | The Software Alliance to Digital Citizen Initiative, Department of Canadian Heritage

# Consultation on the Government's Proposed Approach to Address Harmful Content Online

Submitted via Email to: pch.icn-dci.pch@canada.ca

BSA | The Software Alliance (BSA) welcomes this opportunity to provide comments to the Department of Canadian Heritage regarding the Government's proposed framework for addressing harmful online content (Harmful Content Framework).<sup>1</sup> BSA is the leading advocate for the enterprise software industry domestically and globally.<sup>2</sup> Our members create technologies that power the businesses of other companies and enable the digital transformation of industry sectors across the economy. BSA members provide a range of enterprise software solutions, including cloud infrastructure, customer relationship management software, human resources management programs, identity management services, and online collaboration software. We write today to urge careful consideration about the scope of entities that may be subject to the Harmful Content Framework's core technical requirements.

To help foster a "safe, inclusive, and open online environment," the Harmful Content Framework aims to regulate "social media platforms" to ensure they are acting responsibly to prevent the proliferation of terrorist content, content that incites violence, hate speech,

<sup>&</sup>lt;sup>1</sup> Have your say: The Government's proposed approach to address harmful content online - Canada.ca

<sup>&</sup>lt;sup>2</sup> BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, Zendesk, and Zoom

Machineko - entrele Aple e e entrele des entres estas al antimismo Managenti estas e aple aj al antimismo - antimismo - aple al antimismo - aple aj al antimismo - aple al antimismo al antimismo al antimismo - aple al antimismo al ant

non-consensual intimate imagery, and child sexual exploitation content.<sup>3</sup> To that end, the Harmful Content Framework outlines a series of technical obligations that "Online Communications Services" (OCS) and "Online Communications Service Providers" (OCSP) will be required to adhere to, including: taking "all reasonable measures," including the "use of automated systems" to proactively monitor, identify and remove access to "harmful content" that is "communicated on" the OCS; establishing notice-and-takedown mechanism to enable users of the OCS to flag harmful content that is being made available via the OCS; and, removing (or otherwise render inaccessible) any harmful content within 24 hours of receiving a notification from a user of the OCS.

Given the nature of these obligations, it is vital for the Harmful Content Framework to clearly and carefully define the scope of entities that will be subject to them. As the Discussion Guide notes, the Framework is "intended to capture major platforms, (e.g., Facebook, Instagram, Twitter, YouTube, TikTok, Pornhub)" while excluding organizations that provide "telecommunications" and "technical" services. To that end, the definitions of OCS and OCSP will need to be closely scrutinized to ensure that they align with this vision. The accompanying Technical Paper explains that future legislation will define OCS as a service whose "primary purpose... is to enable users of the service to communicate with other users of the service," and that the term will "exclude services that enable persons to engage only in private communications." With respect to OCSP, the Technical Paper explains the term will exclude telecommunication, information location (i.e., search), hosting, or caching services even in circumstances where "another person uses their services to provide an OCS."

Based on the foregoing, we understand that the Department of Canadian Heritage intends to exclude most business-to-business (B2B) service providers from the scope of the Harmful Content Framework. Such an exclusion will be critical because the Harmful Content Framework's proactive monitoring, automated filtering and takedown requirements would result in a number of unintended consequences if they were extended to B2B services. For instance, requiring B2B cloud providers to proactively monitor and filter for "harmful content" on their enterprise customers' networks would implicate significant privacy and security tradeoffs. BSA members provide B2B cloud services to enterprise customers in every sector of the economy, including the healthcare, banking, energy sectors. Given the sensitivity of their customers' data, enterprise cloud service providers design their systems so that they have limited – if any – visibility into the data they are hosting and/or processing on behalf of their clients. Imposing a filtering requirement on enterprise cloud service providers would thus require them to reengineer their networks in ways that would create significant privacy and security concerns. It could, for instance,

<sup>&</sup>lt;sup>3</sup> Technical paper - Canada.ca

Marchanya, and Angles and Angles and a set for stark and additional stark operational and an end of the the Starking Starks.

prevent enterprise service providers from offering user-controlled encryption protections that are critical to the security of sensitive data.

Extending the 24-hour notice-and-takedown requirement to B2B service providers would likewise create challenges. Consumer-facing online services – including Online Communications Services – are now supported by dozens of backend enterprise services that operate invisibly but play an important role in hosting, optimizing, processing, and routing network communications. For instance, an OCS may utilize an infrastructure-as-a-service provider that hosts its content, a separate registrar to manage its domain, a content delivery network that ensures fast load times around the world, an identity access management provider that controls access to the site, a third-party cybersecurity firm that prevents fraudulent transactions, and many more. While such backend B2B services support the secure and efficient operation of their customer's public-facing services, they generally do not have the technical capacity to remove or disable access to individual pieces of content that may be made available via their customer's services. As a result, if B2B service providers are required to comply with the 24-hour obligation to disable access to content that has been flagged by a member of the public as potentially "harmful," their only recourse would be to cut off services entirely to the OCS.

. . . .

Thank you again for the opportunity to provide initial feedback regarding the proposed Harmful Content Framework.

Seathartel, conservinger et a contra a contra da Paris Sur Contra antenan Municipal contra contra antena y sur contra da Paritana y sur contra da Paritana y Contra da Sur contra da Paritana y s

## CHINESE CANADIAN NATIONAL COUNCIL FOR SOCIAL JUSTICE



# Submission on the Canadian Government's proposed approach to address harmful content online

The Chinese Canadian National Council for Social Justice (CCNC-SJ) is grateful for the opportunity to provide submissions on the government's technical paper on addressing harmful content online (the "Technical Paper").

CCNC-SJ has a 40-year history of advocating for the rights and equal treatment of all in Canada, with a focus on advocating for the interests of the Asian Canadian community and has been particularly outspoken on the issue of online hate. We are pleased to see that many of the <u>recommendations</u>, made in 2020 to the Minister of Canadian Heritage Minister Steven Guilbeault, were incorporated into the Technical Paper.

As Mr. Trudeau's government continues its mandate, we urge them to remember that the threat of online hate is just as urgent today as it was a week ago. CCNC-SJ supports the Technical Paper in principle and commends its drafters on undertaking an ambitious effort to address online hate and social media regulations.

However, the real work must begin now. It is incumbent on the government to make good on its promises and implement an effective and comprehensive scheme to address online hate and social media.

# **Timing and Implementation**

As the COVID-19 Pandemic has taught us, social media can quickly and effectively be used by proponents of hate to disseminate harmful content and misinformation on a massive scale. To date, in collaboration with Professor Ishtiaque Ahmed of UofT, CCNC-SJ has collected over 3,000 anti-Chinese tweets that contain stigmatizing themes or messages, many of which are still available on Twitter.

## No timeline or budget has been established

While CCNC-SJ supports the creation of the three regulatory entities under referred to in the Technical Paper (the Digital Safety Commissioner of Canada, the Digital Council of Canada, and the Advisory Board), we are concerned that no timelines or budgets have been established to enforce these undoubtedly complicated and resource-intensive bodies. There have been implications that it could take months or even years for these bodies to be established. In the meantime, our communities cannot afford to wait, as misinformation and discrimination run amuck on mainstream social media, causing irreparable harm to the reputation and mental health of racialized communities.

Anotherson - concrete sport in a contra a spheric en Proc. And concrete entration Management entrate on concrete in the spirit increase the Provident Contra a

## CHINESE CANADIAN NATIONAL COUNCIL FOR SOCIAL JUSTICE



#### CCNC-SJ recommends that:

- A formal bill immediately is tabled, so that the process for implementing new social media and online hate laws can commence with the inclusion of recommendations made here, and by other community experts.
- The bill must provide flexibility in implementation to accommodate changes in technology and understanding of the spread and appeal of online hate and misinformation.
- A fixed budget and timeline must be provided within the next 3 months to ensure efficacy and proper operation of the regulatory bodies that will be created.

## The advisory board's establishment and role is not transparent

CCNC-SJ acknowledges the acceptance of recommendations to establish an advisory board as part of the regulatory scheme, as well as the criteria that will be used to select individual board members. However, the lack of discretion and transparency for the Minister to select the 7 members of the board is concerning, given that members are appointed by the Minister "at pleasure".

It is unclear who the advisory board is accountable to in their role of overseeing other regulatory bodies, whether they must make reports, and what kind of enforcement or otherwise powers they may have. First and foremost, it is crucial that the individuals who make up the board have the interests of diverse groups in mind and therefore the appointment of the board must be transparent.

#### **CCNC-SJ** recommends that:

- The election of individuals to the advisory board be a public process with clear criteria.
- The role, mandate and powers of the advisory board are clearly articulated and publicly disseminated.

# Weaknesses in the proposal

### The process of removing content is a burden on victims

CCNC-SJ emphasizes that it is not the responsibility of the victim, and those reporting, to remove harmful content. The Technical Paper requires that victims or other interest groups be subjected to potentially lengthy and arduous quasi-judicial processes to have the content removed, adding to their burden, and extending trauma.

As noted above, the COVID-19 Pandemic has demonstrated how quickly harmful content can spread. Moreover, reports and surveys have indicated that victims are not likely to make reports for fear of incurring legal consequences because of distrust in law enforcement and the risk of retaliation and repeating trauma. The balance between the mental health and safety of individuals and the right to freedom of speech is fraught. If content creators and publishers feel so strongly that their content is a lawful exercise of free speech, then the burden should be on them to demonstrate its validity. Instead, it

# CHINESE CANADIAN NATIONAL COUNCIL FOR SOCIAL JUSTICE

Spacharstell, Sonald Spectral Control (1) (1) Control (2) Spectra (2) Control (2) (2) Spectra (2) Control (2) Control (2) (2) Spectra (2) Control (

## CHINESE CANADIAN NATIONAL COUNCIL FOR SOCIAL JUSTICE

CCNC-SJ

is taken on by victims who suffer significantly, and are more likely to be deterred from making reports in the first place.

**CCNC-SJ recommends that:** content identified as harmful or hate speech be removed automatically and that the burden of an appeals process to assess content as legal or not be the responsibility of content creators and/or publishers.

#### The third-party reporting process must be clearly spelled out

Canadian Heritage has indicated that reports can be filed both by victims, as well as organizations representing them, even if such organizations have not been fully retained or authorized to represent them. While this will benefit victims by allowing their interests to be pursued with minimal risk, the process for such representation must be specified in the legislation. Adequate support, guidance, and funding must also be provided to third-party organizations who will have to undertake these undoubtedly daunting and resource-intensive advocacy actions.

**CCNC-SJ recommends that:** various procedural requirements for reporting and third-party reporting be clearly spelled out:

- What the process is and how it is different when third-party organizations report and represent victims.
- Whether victims who are the subject of the third-party reporting process can participate or discontinue a report.
- Whether funding will be provided to community organizations that provide support to or represent victims in removal processes and if so, what the quantum and requirements for receiving funding will be.

#### No uniform reporting system has been suggested

While section 12(a) of the Technical Paper sets out that reporting systems must implement "accessible and easy-to-use flagging mechanisms for harmful content", there are no specifics provided. This will be detrimental to regulators, researchers, and public interest groups who will require uniform data to assess the efficacy of reporting mechanisms, and track trends in online hate and misinformation. It will also be detrimental to users, who may be dissuaded from filing reports due to inconsistent or difficult to access reporting mechanisms.

Indeed, a review of the efficacy of Germany's NETZDG law (one of the world's first and most comprehensive attempts to regulate social media and online hate) revealed that failures to standardize reporting mechanisms and data led to inconsistencies in reports and reported numbers. Comparisons between data sets across platforms are also difficult to analyze. For example, Facebook and Twitter's data focused on the number of complaints (where there could be multiple complaints about a single piece of content), whereas Google provided the number of content items, making it difficult to assess the actual quantity of hateful content across platforms. Facebook also received 100 times less reports

### CHINESE CANADIAN NATIONAL COUNCIL FOR SOCIAL JUSTICE

Скрытичка, сконструкт в оснать с Сефей на Рассобусй салоанного Областий конструкт соверства Пре Ассосо (2) Манитери I Пре

# CHINESE CANADIAN NATIONAL COUNCIL FOR SOCIAL JUSTICE

CCNC-SJ

than Youtube and Twitter despite its wide usage, likely because the reporting function was difficult to find, and required multiple clicks to access.<sup>1</sup>

While CCNC-SJ commends the inclusion of section 14 of the Technical Paper that will require scheduled, detailed reports on various considerations related to online hate and how it is monetized, we repeatedly stress the importance of uniformity in reporting requirements to ensure transparency and accurate comparisons.

**CCNC-SJ recommends that:** a uniform reporting function must be designed and mandated for social media platforms, specifying:

- Location of the reporting function.
- A standardized form and specifications as to what data is collected in the report and provided to regulators.
- Number of clicks necessary to complete the report.

## Enforcement measures aren't stringent enough

CCNC-SJ believes that the enforcement measures proposed for repeated non-compliance with orders to remove child exploitation and terrorist content should be extended to hate speech and misinformation. This would mean that social media platforms may be at risk of being blocked in whole or in part by internet service providers should they repeatedly fail to comply with orders to remove hate speech and misinformation.

Hate speech has no place in Canada, and the NETZDG law has demonstrated that social media companies can act much quicker in removing content than they claim. In Germany, Facebook hired several thousand more content moderators and can provide detailed country-wide reports.<sup>2</sup> We also learned from the NETZDG law that social media companies are more than happy to pay fines to underreport hate speech, even when the fines are in the range of 2 million Euros.<sup>3</sup>

It is important to recognize that any financial penalty, even up to significant fines of \$20-25 million or 4-5% of global revenues for offences by social media companies, may ultimately result in a pay-to-play system, where social media companies consider fines as simply part of the cost of doing business. While the fines set out in the Technical Paper are admirable, they pale in comparison to social media companies' potential earnings. The anti-vax industry for example, is estimated to generate Facebook \$1

<sup>&</sup>lt;sup>1</sup> https://www.ivir.nl/publicaties/download/NetzDG Tworek Leerssen April 2019.pdf

<sup>&</sup>lt;sup>2</sup>https://static1.squarespace.com/static/5ea874746663b45e14a384a4/t/5fd76fe7e5ac582896424816/1607954415 617/MTD\_Report\_Tenove\_Tworek.pdf

<sup>&</sup>lt;sup>3</sup> https://www.politico.eu/article/germany-fines-facebook-e2-million-for-violating-hate-speech-law/

Construction of the construction of the control of the first star Proceeding of Continuous deterministic of the construction of the start of the control of the start of

# CHINESE CANADIAN NATIONAL COUNCIL FOR SOCIAL JUSTICE



billion in advertising revenues a year, making even fines in the tens of millions negligible by comparison.<sup>4</sup>

It is also important to note that if the government uses fines, in whole or in part, to deter social media companies, then part of that revenue from the fines should be used to heal and benefit the communities that online hate and misinformation target and harm.

#### CCNC-SJ recommends that:

- Social media companies face the potential penalty of being blocked in whole or in part in Canada for persistent failure to adhere to orders to remove online hate and misinformation.
- Social media companies be subject to higher fines for punishable offences.
- The government commits revenue from fines to support disadvantaged communities, victims, and organizations combating online hate and misinformation.

## The role of the police is still unclear and should be handled with caution

The Technical Paper outlines extensive and far-reaching powers of the police to gather information on proponents of online hate and misinformation.

Police involvement in the prosecution and removal of online hate and misinformation must be done with extreme caution. Disadvantaged communities have a tumultuous relationship with law enforcement, particularly concerning hate crimes and hate speech. Current police training and guidelines are underdeveloped to tackle real time incidents of hate and they will also face incredible challenges in prosecuting and handling online hate speech cases.

There must be measures of accountability with clear guidelines, boundaries, and training for the police to play a role in the fight against online hate.

#### CCNC-SJ recommends that:

- Community organizations are provided with the opportunity and funding to provide oversight.
- Extreme caution is exercised when integrating the police into the regulation of online hate and social media.
- Standardized training on dealing with hate crimes and hate speech be provided to police across Canada.
- Clear guidelines and boundaries are established for the role of police and the extent of their powers.

## CHINESE CANADIAN NATIONAL COUNCIL FOR SOCIAL JUSTICE

<sup>4</sup> https://252f2edd-1c8b-49f5-9bb2-

cb57bb47e4ba.filesusr.com/ugd/f4d9b9 6910f8ab94a241cfa088953dd5e60968.pdf

Marchandel, Conservation Processing on Conservation Processing Conservation Management Conservation Conservation Processing Cons

## CHINESE CANADIAN NATIONAL COUNCIL FOR SOCIAL JUSTICE



# **Research and adaptation**

The proposed social media legislation will undoubtedly encounter a litany of social and technological hurdles and inefficacies along the way. The Technical Paper appears to require the provision of accessible, comprehensive data that can better help shape public policy on online hate and social media. Research is crucial and must be conducted continuously with mechanisms put in place to expeditiously adapt regulations based on said research.

# Understanding the algorithms

One thing we know for certain is that social media platforms and their algorithms, like Instagram, recommend posts containing misinformation, resulting in hundreds of thousands of likes.<sup>5</sup>

There are robust requirements for public transparency and reporting in the Technical Paper, but notably missing is the requirement for social media to disclose information on their algorithms and how they work. While there is some loose wording that inspectors can examine computer algorithms under section 89 of the Technical Paper, the extent of this power is unclear and doesn't guarantee that inspectors will have the skills and expertise to understand the algorithms without enforcing their own implicit biases. Data on the algorithms must be publicly accessible and comprehensive for research purposes. Social media algorithms are undoubtedly complicated and will require significant resources to understand and analyze.

How regulatory bodies will be able to analyze and ensure full disclosure from social media companies is not clear, which is fatal to any attempts to regulate these companies who will undoubtedly resist disclosure obligations.

If the government is unable to lay out a comprehensive plan as to how it will compel full disclosure of how social media algorithms work, it is incumbent for the government to invest in third-party resources and research that aim to understand these algorithms, like that conducted by CCNC-SJ.

#### CCNC-SJ recommends that:

- Social media companies are required to disclose how their algorithms work.
- The government provide funding to organizations researching social media algorithms and the spread of online hate and misinformation.

5 https://252f2edd-1c8b-49f5-9bb2-

cb57bb47e4ba,filesusr.com/ugd/f4d9b9\_9877528dd81b402b948044ab10a989d9.pdf

# CHINESE CANADIAN NATIONAL COUNCIL FOR SOCIAL JUSTICE

Department commensation and writing of Lot sur Particley & Participantian Obcurrent introduce of consumer, It the Receipt to Hantmenther Lars

## CHINESE CANADIAN NATIONAL COUNCIL FOR SOCIAL JUSTICE



#### Content Removals cannot be the only measure of efficacy

Content removals are a problematic measure of success. Though it may be beneficial to see the removal of hate content increase over time, this does not necessarily indicate success in fighting hate speech. Instead, it may indicate an increase in hate speech or incentivization of its creation.<sup>6</sup>

The measure of success of Canada's legislation against online hate and misinformation is likely to change as we come to better understand social media algorithms, the scale of online hate and misinformation, and how people respond to legislation and regulation.

It is crucial that any social media legislation that is tabled provides for regulations that are flexible and have space and mechanisms for amendments based on further research.

#### CCNC-SJ recommends that:

- More research is conducted and organizations conducting research are provided with adequate funding to perform research on a continued basis.
- The regulations that are a part of the legislation are adaptable and provides space for amendments in policy to reflect further research and findings, as well as better measures of efficacy.

- 30 -

<sup>6</sup><u>https://static1.squarespace.com/static/5ea874746663b45e14a384a4/t/5fd76fe7e5ac582896424816/1607954415</u> 617/MTD Report Tenove Tworek.pdf

# CHINESE CANADIAN NATIONAL COUNCIL FOR SOCIAL JUSTICE

# (III) RANKING DIGITAL RIGHTS

September 24, 2021

Honorable members of the Department of Canadian Heritage:

Ranking Digital Rights (RDR) welcomes this opportunity for public consultation on the Canadian government's proposed approach to regulating social media and combating harmful content online. We work to promote freedom of expression and privacy on the internet by researching and analyzing how global information and communication companies' business activities meet, or fail to meet, international human rights standards (see <u>www.rankingdigitalrights.org</u> for more details). We focus on these two rights because they enable and facilitate the enjoyment of the full range of human rights comprising the Universal Declaration of Human Rights (UDHR), especially in the context of the internet.<sup>1</sup>

RDR broadly supports efforts to combat human rights harms that are associated with digital platforms and their products, including the censorship of user speech, incitement to violence, campaigns to undermine free and fair elections, privacy-infringing surveillance activities, and discriminatory advertising practices. But efforts to address these harms need not undermine freedom of expression and information or privacy. We have long advocated for the creation of legislation to make online communication services (OCSs) more accountable and transparent in their content moderation practices and for comprehensive, strictly enforced privacy and data protection legislation.<sup>2</sup>

We commend the Canadian government's objective to create a "safe, inclusive, and open" internet. The harms associated with the operation of online social media platforms are varied, and Canada's leadership in this domain can help advance global conversations about how best to promote international human rights and protect users from harm. As drafted, however, the proposed approach fails to meet its stated goals and raises a set of issues that jeopardize freedom of expression and user privacy online. We also note that the framework contradicts commitments Canada has made to the Freedom Online Coalition (FOC)<sup>3</sup> and Global Conference for Media Freedom,<sup>4</sup> as well as previous work initiating the U.N. Human Rights

<sup>&</sup>lt;sup>1</sup> https://www.un.org/en/about-us/universal-declaration-of-human-rights.

<sup>&</sup>lt;sup>2</sup> https://rankingdigitalrights.org/index2020/recommendations.

<sup>&</sup>lt;sup>3</sup> https://freedomonlinecoalition.com/aims-and-priorities/;

https://www.international.gc.ca/campaign-campagne/media\_freedom-liberte\_presse-2020/global\_pledgeengagement\_mondial.aspx?lang=eng.

Council's first resolution on internet freedom in 2012.<sup>5</sup> As Canada prepares to assume the chairmanship of the FOC next year, it is especially important for its government to lead by example. Online freedom begins at home. As RDR's founder Rebecca MacKinnon emphasized in her 2013 FOC keynote speech in Tunis, "We are *not* going to have a free and open global Internet if citizens of democracies continue to allow their governments to get away with pervasive surveillance that lacks sufficient transparency and public accountability."<sup>6</sup>

Like many other well-intentioned policy solutions, the government's proposal falls into the trap of focusing exclusively on the moderation of user-generated content while ignoring the economic factors that drive platform design and corporate decision-making: the targeted-advertising business model. In other words, restricting specific types of problematic content overlooks the forest for the trees. Regulations that focus on structural factors—i.e., industry advertising practices, user surveillance, and the algorithmic systems that underpin these activities—are better suited to address systemic online harms and, if properly calibrated, more sensitive to human rights considerations.<sup>7</sup>

In this comment we identify five issues of concern within the proposal and a set of policy recommendations that, if addressed, can strengthen human rights protections and tackle the underlying causes of online harms.

#### Issues of Concern and Recommendations

1. Proposed regulatory bodies have expansive powers and limited oversight. RDR is concerned with the sweeping authority vested in the new regulators of online content moderation (Module 1(C): Establishment of the new regulators; Module 1(D): Regulatory powers and enforcement). Particularly troubling are the provisions that empower regulators to define new categories of harmful content for future inclusion under the framework (Module 1(A) #9) and the rule that enables the government to order country-wide ISP blocking of non-compliant OCSPs (Module 1(D) #120). Such broad regulatory powers are inconsistent with the principles of necessity and proportionality that must underlie restrictions on fundamental human rights.<sup>8</sup> While Canadians can take comfort in the strength of their democratic institutions, all countries are but one election away from democratic decline and a slide into authoritarianism. Our recent experience in the United States has been a sobering one, reinforcing the importance of balanced institutional powers, good governance, and oversight mechanisms.

5

7

https://www.international.gc.ca/world-monde/issues\_development-enjeux\_developpement/human\_rightsdroits\_homme/internet\_freedom-liberte\_internet.aspx?lang=eng;

https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement. <sup>6</sup> https://consentofthenetworked.com/2013/06/17/freedom-online-keynote/.

https://rankingdigitalrights.org/wp-content/uploads/2020/07/Its-the-Business-Model-Executive-Summary-R ecommendations.pdf.

<sup>&</sup>lt;sup>8</sup> https://www.ohchr.org/documents/issues/privacy/electronicfrontierfoundation.pdf

**Recommendation:** Engage civil society for guidance on how to implement provisions that protect human rights. As numerous public critiques of the Government's framework have made clear,<sup>9</sup> strong civil society involvement is necessary to help define appropriate statutory limitations and bolster human rights protections in the proposed legislation. Specifically, an independent body of civil society stakeholders should be consulted by the government to provide direct input on appropriate reforms. These consultations should themselves be public and transparent.

**Recommendation:** Ensure effective and independent oversight. Any government bodies empowered to flag content for removal by companies, or empowered to require the blockage of services, or to compel network shutdowns, must be subject to robust, independent oversight and accountability mechanisms to ensure that the power to compel companies to restrict online speech, suspend accounts, or shut down networks is not abused in a manner that violates human rights.

2. Little attention given to human rights considerations. Despite a stated desire to safeguard "fundamental freedoms and human rights" (Module 1(A) #1(h)), the Technical paper does not enumerate the specific values being protected, the mechanisms by which this might occur, nor the tradeoffs involved in securing some rights at the expense of others (i.e., protecting users from online harm versus limiting online expression).

<u>Recommendation</u>: Evaluate the human rights impacts of the proposed legislation. Both state and non-state actors have human rights obligations. Protecting these rights must start with the Canadian government, which should conduct and publish an independent Human Rights Impact Assessment (HRIA) of the proposal.

**Recommendation:** Require companies to undertake independent assessments of the human rights impacts of their content moderation practices. As part of new reporting obligations (Module 1(B) #14, #20), OCSs should be obligated to conduct independent assessments of potential human rights impacts that could occur in relation to the operation of their platform, service, or devices and to take the findings of such assessments into account when making business decisions. The process for conducting these assessments and acting on them should be made public. Human Rights Impact Assessments accord with the UN Guiding Principles on Business and Human Rights, which detail the human rights responsibilities of governments and companies alike.<sup>10</sup>

- 24-hour takedown requirements for content will lead to unnecessary censorship. The obligation that OCSs must take action on content flagged as infringing (Module 1(B), #10-12) within 24 hours is particularly onerous and harmful to freedom of expression. This provision is similar to those found in other efforts to regulate online speech, most
- 9

https://ablawg.ca/2021/09/13/the-federal-governments-proposal-to-address-online-harms-explanation-and -critique/; https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/

<sup>&</sup>lt;sup>10</sup> https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\_EN.pdf.

notably, Germany's Network Enforcement Act (NetzDG). NetzDG has become a model for internet regulations in more authoritarian states,<sup>11</sup> inspiring laws and proposals in places such as Russia, Venezuela, Vietnam, and Turkey.<sup>12</sup> Timed takedown mandates have received broad criticism from academic experts<sup>13</sup> and civil society groups<sup>14</sup> for their likelihood to censor lawful speech.

**Recommendation:** Remove 24-hour takedown requirements. In addition, complainants requesting content removals should provide additional information, including justification for the removal, the Internet identifier and an explanation of the content, inclusion of possible defenses open to the user content provider, and a statement that the request was made in good faith. These guidelines are drawn from the Manila Principles for intermediary liability standards.<sup>15</sup>

4. Proactive content monitoring threatens user privacy. The current structure of the proposal all but ensures that OCSs will implement proactive monitoring tools (i.e., algorithmic filtering software) to moderate illegal content (Module 1(B) #10).<sup>16</sup> Proactive filtering regimes of this kind have been identified by the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression as "inconsistent with the right to privacy and likely to amount to pre-publication censorship."<sup>17</sup> Moreover, automated content moderation systems have been found to disproportionately burden marginalized communities.<sup>18</sup> Belief in the magic of artificial intelligence (AI) to solve harmful content problems at scale is deeply problematic. Algorithmic moderation approaches are subject to significant limitations<sup>19</sup> due to their inability to comprehend contextual elements of speech, biased datasets that

11

13 https://www.ivir.nl/publicaties/download/NetzDG Tworek Leerssen April 2019.pdf;

https://www.hiig.de/wp-content/uploads/2018/07/SSRN-id3216572.pdf;

http://justitia-int.org/en/the-digital-berlin-wall-how-germany-created-a-prototype-for-global-online-censorsh jp/.

ip/. <sup>12</sup> https://www.eff.org/deeplinks/2020/07/turkeys-new-internet-law-worst-version-germanys-netzdg-yet.

https://www.lawfareblog.com/rushing-judgment-examining-government-mandated-content-moderation.

https://www.article19.org/wp-content/uploads/2018/07/Germany-Responding-to-%E2%80%98hate-speec h%E2%80%99-v3-WEB.pdf;

https://edri.org/our-work/eu-action-needed-german-netzdg-draft-threatens-freedomofexpression/; https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law;

https://blog.mozilla.org/netpolicy/2019/03/07/one-hour-takedown-deadlines-the-wrong-answer-to-europescontent-regulation-question//

<sup>&</sup>lt;sup>15</sup> <u>https://manilaprinciples.org/principles.html</u>.

https://techpolicy.press/five-big-problems-with-canadas-proposed-regulatory-framework-for-harmful-online -content/.

<sup>&</sup>lt;sup>17</sup> https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/ContentRegulation.aspx.

<sup>18</sup> https://aclanthology.org/P19-1163.pdf;

https://cdt.org/wp-content/uploads/2017/12/FAT-conference-draft-2018.pdf;

https://www.newamerica.org/oti/reports/everything-moderation-analysis-how-internet-platforms-are-usingartificial-intelligence-moderate-user-generated-content/the-limitations-of-automated-tools-in-content-mode ration/

<sup>&</sup>lt;sup>19</sup> https://www.ivir.nl/publicaties/download/Al-Llanso-Van-Hoboken-Feb-2020.pdf.

discriminate against users and their content, and inaccuracies associated with predictive models.<sup>20</sup>

<u>Recommendation</u>: Eliminate broad obligations to monitor for harmful content. The government should consult with civil society stakeholders to craft an approach that is narrower in scope and more proportionate to the desired aim. (See the Manila Principles for guidance on the creation of intermediary liability standards that align with international human rights standards.)<sup>21</sup>

<u>Recommendation</u>: Require companies to demonstrate algorithmic accountability. Algorithmic systems are integral to the operation of OCSs' content moderation and content delivery functions. Yet, these tools remain largely hidden from public scrutiny and oversight. At a minimum, the government should mandate that companies follow international human rights standards in developing and using algorithms (see the recommendations from our 2020 Corporate Accountability Index for further guidance on this issue).<sup>22</sup> In addition, they should require OCSs to make public comprehensive and comprehensible policies describing how algorithms are developed and used across their services, especially in relation to the moderation of user and advertising content. As we found in our 2020 Corporate Accountability Index, only four digital platforms provided any information about the human rights impacts of their automated systems<sup>23</sup> and no services offered user access to algorithmic system development policies.<sup>24</sup>

5. Regulating specific content overlooks how business models facilitate online harms. Content restrictions, without substantive consideration of the economic and technical systems that facilitate content delivery, are inadequate solutions to combat online harms. Instead, legislative attention must center on business models based on the mass collection and monetization of user data for targeted advertising.<sup>25</sup> These industry practices facilitate a range of human rights abuses, most immediately those related to privacy, freedom of expression and information, and protection from discrimination.<sup>26</sup>

<u>Recommendation</u>: Focus regulation on the targeted-advertising business model. In particular, companies should be required to disclose information that demonstrates they are tracking the social impact of their targeted-advertising and algorithmic systems, taking necessary steps to mitigate risk and prevent social harm. Additionally, company

<sup>26</sup> https://rankingdigitalrights.org/its-the-business-model/;

<sup>20</sup> 

https://www.newamerica.org/oti/reports/everything-moderation-analysis-how-internet-platforms-are-usingartificial-intelligence-moderate-user-generated-content/.

<sup>&</sup>lt;sup>21</sup> https://manilaprinciples.org/principles.html.

<sup>22</sup> https://rankingdigitalrights.org/index2020/recommendations.

<sup>23</sup> https://rankingdigitalrights.org/index2020/indicators/G4d.

<sup>24</sup> https://rankingdigitalrights.org/index2020/indicators/P1b.

<sup>&</sup>lt;sup>25</sup> https://datasociety.net/wp-content/uploads/2018/10/DS\_Digital\_Influence\_Machine.pdf.

https://www.amnesty.org/en/documents/pol30/1404/2019/en/;

https://www.ohchr.org/Documents/Issues/Business/B-Tech/B\_Tech\_Foundational\_Paper.pdf.

transparency and reporting obligations should be expanded to cover content moderation practices for advertisements (see the recommendations from our 2020 Corporate Accountability Index for further guidance on this issue).<sup>27</sup> Our research in 2020 concluded that although most companies provide at least partial disclosure about their advertising content and targeting policies,<sup>28</sup> the majority do not disclose any information about changes to these policies nor changes to their advertising targeting policies.<sup>29</sup>

**Recommendation:** Require disclosure about data inference used for advertising purposes. Algorithms require large amounts of user data to make decisions related to various platform services. However, service users know little about how their personal data informs such processes, particularly for targeted advertisement purposes. The government should require that companies provide users with access to this information, including any information used to make inferences or predictions about them, in a structured format. As we determined in our 2020 Index, many digital platforms fail to disclose what information they infer and how.<sup>30</sup> The material for the ones that do is extremely limited.

**Recommendation:** Strengthen legal provisions for data-minimization, purpose limitation, and personal control—and enforce them. Privacy regulations should protect users from the harmful effects of OCSs' targeted advertising practices by prohibiting companies (as well as other actors, including government agencies) from collecting information that is not strictly necessary to provide the service requested by the user, absent user consent. Using such information for a different purpose than that for which it was collected without the consent of the affected individual should likewise be prohibited. Moreover, individuals should not be able to opt-in to discriminatory advertising or to the collection of data that would enable it. Our research shows that across the online ecosystem, companies provide little transparency about how users can control and limit the ways their data are used.<sup>31</sup>

The nature and severity of harms stemming from the operation of online communication services grows increasingly problematic. This requires the state to play a stronger role overseeing industry activities. But governments must establish a modern regulatory approach marked by transparency, civil society engagement, heightened concern for human rights, and other ingredients consistent with best practices in the governance field. Without these guidelines, efforts to safeguard freedom of expression, user privacy, and other rights and freedoms will inevitably fall flat.

 <sup>27</sup> https://rankingdigitalrights.org/index2020/recommendations.
 <sup>28</sup> https://rankingdigitalrights.org/index2020/indicators/F1b; https://rankingdigitalrights.org/index2020/indicators/F1c.
 <sup>29</sup> https://rankingdigitalrights.org/index2020/indicators/F2b; https://rankingdigitalrights.org/index2020/indicators/F2c.

<sup>&</sup>lt;sup>30</sup> https://rankingdigitalrights.org/index2020/indicators/P3b.

<sup>&</sup>lt;sup>31</sup> https://rankingdigitalrights.org/index2020/indicators/P7.

We strongly caution against further content regulation. Such approaches will always be an imperfect solution for the problem of harmful material online, one that is neither comprehensive in scope, nor free from error and possible corruption. They also set a troubling precedent as a template that countries with less respect for human rights may choose to emulate, with grave consequences for free expression and other rights. Instead, as we have recommended, regulations should target the underlying economic systems—targeted advertising business models, indiscriminate user surveillance, and unaccountable algorithms— that have contributed to some of the worst abuses of online speech.

Canada's strong history of support for civil liberties and internet freedom well positions it to chart a new global path on these issues. In doing so the government can uphold its obligation to protect the fundamental human rights of its own citizens and residents, establish new standards of democratic accountability and transparency over social media platforms, and become a champion for internet users around the world.

Thank you again for the opportunity to participate in this consultation. We look forward to engaging further with the Canadian government and its representatives on these matters. We can be reached by email at policy@rankingdigitalrights.org.

Sincerely,

Jessica Dheere, Director Nathalie Maréchal, PhD, Senior Policy & Partnerships Manager Alex Rochefort, Policy Fellow

Analysis and a second s



The Committee for Justice in Canada B'NAI BRITH CANADA Le comité pour la justice au Canada

Government of Canada Consultations on Online Harms Submission from B'nai Brith Canada September 24, 2021

These views are preliminary in nature, intended to focus on general principles and objectives. Should the consultation process be restarted, we will offer additional, detailed views on the proposals to be advanced by the Government of Canada.

#### Introduction

B'nai Brith Canada is a national organization in existence since 1875, advocating for the interests of the grassroots Jewish community. Together with our League for Human Rights and Committee for Justice in Canada, a key focus of our work is combatting antisemitism, hate crimes and hate speech, and fostering Jewish life in Canada.

This submission is not tabula rasa. Our views have been conveyed to government and parliament over several years, including, inter alia, through evidence before the House of Commons Standing Committee on Canadian Heritage during its study of steps needed to address systemic racism and religious discrimination (Motion M-103). In May, 2019, we testified before the House of Commons Standing Committee on Justice and Human Rights, and we have carefully assessed the recommendations in that Committee's report of June, 2019, "Taking Action to End Online Hate".

B'nai Brith has provided testimony to both the <u>Canadian Commission</u> on Democratic Expression (October, 2020) and the <u>Interparliamentary Task Force</u> to Combat Online Antisemitism (November, 2020). Separately, we have submitted <u>detailed views</u> to the Department of Justice (August, 2020).

Secretaria - constany a secretaria e Electro I a Secretaria decempiation - constanta a secondaria de transmissiones de las

#### Page Two

### The Overriding Objective

Freedom of religion is a value inherently associated with the right to freedom from incitement to hatred. In that context, freedom of expression must have no greater weight than the right to freedom from incitement to hatred. The defence of religious expression must trump the offence of incitement to hatred. The right to freedom from hatred because of one's religion must exist on the same plane as freedom of expression. The latter cannot be considered of a higher order.

Striking a balance between the right to freedom of expression and the right to freedom from incitement to hatred and discrimination requires remedies which are not so easy of access that they can become vehicles to harass legitimate expression. They also cannot be so difficult of access that they are effectively unworkable. This underlying objective must be reflected in any new proposals to deal with online harms.

#### The Importance of Definitions

In order to appreciate incitement to hatred, and to consider it within the framework of freedom of expression, it is important to have working definitions relevant to targets of hate or victim groups. Clear definitions are of fundamental importance in assessing whether words constitute acceptable free speech or incitement to hatred. This is why B'nai Brith Canada supports the more widespread adoption and implementation of the non-legally binding working <u>definition of antisemitism</u> used by the International Holocaust Remembrance Alliance (IHRA). This definition has been adopted by the Government of Canada; that adoption must be reflected in any new proposals to deal with online harms.

#### Hate Speech

The discussion framework identifies hate speech as one of the five categories of harmful content. **Our presumption is that the definition of harmful hate speech content will be harmonized with the proposed definition in Bill C-36**. We look forward to having input on that definitional framework in any renewed consideration of Bill C-36.

It is important that there be thorough consultation in the proposed addition of 'hated' for the two hate propaganda offences in Section 319 of the *Criminal Code*.

.../3

## Page Three

We welcome proposals in Bill C-36 to enact an improved version of Section 13 of the Canadian Human Rights Act, which will define a new discriminatory practice of communicating hate speech online. B'nai Brith Canada has previously testified before Parliament on the challenges of the old Section 13, offering ideas on content for any newly reconstituted Section. We look forward to being involved in consultations on this element as it is regarded an essential piece of the framework to address online harms.

The discussion framework seems to address dealing with hate speech entirely in a criminal context; that is, focusing in a more weighted fashion on the roles to be played by Canada's national security agencies – 'options to alert law enforcement and CSIS of certain forms of harmful content under the five categories'. B'nai Brith Canada believes that the online harms framework must be seen as appropriately balanced between policy tools to take down harmful content that poses a social cohesion challenge and law enforcement actions when there is an imminent risk of serious harm or criminal activity.

## **Terrorism Content**

The discussion framework addresses 'terrorist content' as another element of harmful content. There is an **essential requirement to also incorporate advocating or promoting terrorism**, as B'nai Brith Canada argued in its Parliamentary testimony regarding Bill C-59, and the proposal to remove the offence of advocating or promoting terrorism from the *Criminal Code* and to replace it with the offence of counselling terrorism.

The proposed **online harms framework can give substance to the case for addressing the advocacy or promotion of terrorism** in a new policy space. By addressing the online dimension, the Government of Canada can rightly signal that the prosecution of incitement to terrorism, within Crown investigation and prosecution offices, is to be given a higher priority; that here needs to be more resources, more expertise, and more training applied.

### **Consultative Mechanisms and Processes for Public Input**

We welcome the proposed creation of a *Digital Safety Commission*, intended to support three bodies: the Digital Safety Commissioner of Canada, the Digital Recourse Council of Canada, and the Advisory Board to support both. These **new regulatory bodies must include a clear process of consultation with communities most affected** by harmful online content and the **consultation should be ongoing**, **not just reactive or in response to individual challenges**.

## Page Four

In the past, B'nai Brith Canada has argued for creation of a forum similar to the Canadian Broadcast Standards Council, to convene social media companies, civil society, and other stakeholders – in this case, representatives of the Jewish community – to develop and implement codes of conduct to address harmful speech. The involvement of religious communities most affected by harmful online content is essential (i.e., in addition to 'equity, regional and language groups').

### Addressing Disinformation

B'nai Brith Canada has testified before Parliament, and several bodies (such as the Interparliamentary Task Force to Combat Online Antisemitism and the Network Contagion Research Institute) have emphasized, that hate speech is only part of the problem. A considerable amount of disinformation and conspiracy theories are not hate speech but must be considered within the online harms framework; that is, it is exceptionally dangerous speech even if it is not hate. In addition, there is a considerable amount of hateful speech on social media that does not rise to the level of criminal speech.

The Government of Canada online harms framework must address the problem of disinformation. In so doing, the proposals offered do seem to acknowledge that social media platforms cannot be left to address disinformation on their own. B'nai Brith Canada also subscribes to the view that governments are not best placed to control platforms in the area of disinformation. There is a clear role for the Digital Safety Commission in this space.

We are attracted to the ideas of those supporting the need for a new institution to combat disinformation. Funded by government, industry and civil society, such an institution would report to Parliament but remain independent in its decisions and be staffed by experts with knowledge of substance and cultural viewpoints, using technology as a tool to track disinformation and assess its impact.

### Education

B'nai Brith Canada has welcomed Canada's signature of the 'Christchurch Call to Action' and the announcement of a <u>'Digital Charter'</u>. We have advocated or clear measures to develop further and implement these instruments in the Canadian context in close consultation with Jewish community organizations.

..../5

## Page Five

Canada's Digital Charter includes a welcome **Principle #9 that says our networks should be free from hate and violent extremism**, that "Canadians can expect that digital platforms will not foster or disseminate hate, violent extremism or criminal content." But the Charter does not seem to develop that theme in detail. Now is the time to do so. We see the Department of Justice questions as working towards that goal.

B'nai Brith Canada recommends a **re-purposing of current programmes and funding envelopes related to digital literacy to create resources specifically focused on countering online hate**, particularly that of an antisemitic nature, and that those resources be applied both by government of Canada agencies and the *Digital Safety Commission*.

We need to focus on hate content, before it transforms into terrorist and violent extremist content online. In December 2018, the Government of Canada launched the <u>National Strategy on Countering Radicalization to Violence</u>, which outlines Canada's approach and priorities to prevent the kind of radicalization that leads to violence. Within this strategy, we need to focus more on how online hate, countered at an early stage, can help forestall radicalization to violence.

The Digital Safety Commission, in close consultation with groups seriously affected by harmful online content, should address **the priority need for 'counter speech' initiatives**, including fostering, aggregating and promoting positive messages responding to offensive content. (See, also, our proposals on countering disinformation, above).

The online harms framework should also address how the Government of Canada and the *Digital Safety Commission* can work with the Canadian Human Rights Commission, and provincial human rights commission, to **further develop a public education mandate that would focus on understanding, reporting, and countering online hate and antisemitism.** 

## A Right of Individual Redress

The online harms framework must **ensure that individuals have a clear right of complaint and redress** when impacted by harmful content. The framework should focus on the **need to expand tools and services for targets**. Platforms should offer far more user-friendly services, tools, and opportunities for individuals facing or fearing online attack. This includes greater filtering options that allow individuals to decide for themselves how much they want to see of likely hateful comments.

. . ./6

## Page Six

There needs to be **protections for individuals who are being harassed** in a coordinated way, including user-friendly tools to help targets preserve evidence and report problems to law enforcement and platforms.

## The 'Trusted Flagger' Approach

In November, 2017, we wrote Ministers regarding the <u>European Union's May 31, 2016</u>, <u>Code of Conduct on Illegal Online Hate Speech</u>, and suggested **Canada adopt the EU's 'trusted flagger' approach** as one measure in addressing online hate. We have made this same point in testimony to parliamentarians. In theory, the major service providers prohibit, under their terms of service, incitement to hatred; it is worthwhile making an effort to turn this prohibition in theory into prohibition in practice.

The **Digital Safety Commission could and should develop a similar agreement** with the major internet providers and develop its own list of 'trusted flaggers' to engage in similar work. The work should be coordinated with the European Commission and the European 'trusted flaggers' to avoid duplication of effort.

## Addressing Uninformed Deplatforming

Deplatforming is a very simple, indeed somewhat simple-minded phenomenon. It is essentially a means of political protest and activism that involves denying specific forums — usually but not always of the prestigious variety — to certain speakers or movements. This means things like disinviting or picketing speakers, disrupting events (sometimes violently), pushing social media companies to ban offensive accounts and, perhaps most effectively, convincing companies and corporations to fire people who engage in offensive speech or espouse offensive ideas.

Applying specific definitions, such as the IHRA definition of antisemitism, through a legislative and policy framework, would help address the illegitimate use of deplatforming as a mechanism to curtail freedom of expression.

### Social Media Transparency

B'nai Brith Canada has noted two particular pieces of United States legislation that merit consideration as Canada's online harms framework takes shape.

### Page Seven

Legislation from California State Assembly member Jesse Gabriel would require social media platforms to publicly disclose their content moderation policies regarding online hate/racism, disinformation, extremism, harassment and foreign interference, as well as key metrics and data around the enforcement of their policies.

<u>Assembly Bill 587, the Social Media Transparency and Accountability Act of 2021,</u> seeks to address the ways in which social media foments hate speech, disinformation, conspiracy theories, and violent extremism that allows for the harassment and targeting of traditionally marginalized groups.

At the federal level, Congressman Tom Malinowski and Congresswoman Anna G. Eshoo have reintroduced the *Protecting Americans from Dangerous Algorithms Act*, legislation to hold large social media platforms accountable for their algorithmic amplification of harmful, radicalizing content that leads to offline violence.

The bill narrowly amends Section 230 of the *Communications Decency Act* to remove liability immunity for a platform if its algorithm is used to amplify or recommend content directly relevant to a case involving interference with civil rights; neglects to prevent interference with civil rights; and in cases involving acts of international terrorism. The text of the draft legislation is <u>here</u>.

Accessing comments of the terminal of the EE conference of the terminal of the operation of the terminal of the terminal defension of the terminal of the

Government of Canada

Office of the Federal Ombudsman for Victims of Crime

240 Sparks Street P.O. Box 55037 Ottawa, ON K1P 1A1 Gouvernement du Canada

Bureau de l'ombudsman fédéral des victimes d'actes criminels

240, rue Sparks C.P. 55037 Ottawa (Ontario) K1P 1A1

## Submission to the Department of Canadian Heritage on the Proposed Approach to Address Harmful Content Online

Submitted by:

Ms. Heidi Illingworth, Ombudsman Office of the Federal Ombudsman for Victims of Crime September 2021

ABOUT THE OFFICE OF THE FEDERAL OMBUDSMAN FOR VICTIMS OF CRIME

The Office of the Federal Ombudsman for Victims of Crime helps victims to address their needs, promotes their interests and makes recommendations to the federal government on issues that affect victims. For more information visit: www.victimsfirst.gc.ca

Madhardd - caladachfa co collar Glei - Che Chel - an dhlaan Maranal aha - collar an dhlaan Maranal aha - collar ahar

## ADDRESSING HARMFUL CONTENT ONLINE

Submission on the Government's proposed approach to make social media platforms and other online communications services more accountable and more transparent when it comes to combating harmful content online.

## Context

As Federal Ombudsman for Victims of Crime, my mandate is to help ensure the rights of victims and survivors of crime are respected and upheld, and that the federal government meets its obligations to victims. In addition to assisting individual victims, I also have a responsibility to identify and bring forward emerging and systemic issues that negatively affect victims and survivors of crime at the federal level.

## Introduction

In June 2021, the Minister of Justice introduced Bill C-36: An Act to amend the Criminal Code and the Canadian Human Rights Act and to make related amendments to another Act (hate propaganda, hate crimes and hate speech) in the House of Commons. The intention of Bill C-36 was to amend the Criminal Code to create a recognizance to keep the peace relating to hate propaganda and hate crime and to provide a definition for "hatred".

Now the Government of Canada is proposing a new approach to regulating social media and combating harmful content online. The purpose of the approach is to hold entities accountable to regulate online harmful content. The proposed legislation would apply to online communication service providers (e.g., Instagram, TikTok, Twitter, Facebook, Pornhub), and exclude private communications and telecommunications service providers. The proposed legislation would target five categories of harmful content: terrorist content; content that incites violence, hate speech, non-consensual sharing of intimate images, and child sexual exploitation content. The legislation would create a new Digital Safety Commission of Canada, comprised of three bodies (the Digital Safety Commissioner of Canada, the Digital Recourse Council of Canada, and an Advisory Board), to operationalize, oversee and enforce the new system.

## Position

In my view, it is critical that a new legislative and regulatory framework be developed to require Online Content Service Providers to take all reasonable measures to identify harmful content that is communicated on their platform and to make that harmful content inaccessible to persons in Canada. There must be accountability for victims.

In August 2020, the OFOVC provided a <u>submission</u> to the consultation on Online Hate conducted by the Justice Committee. The main premise of the submission was that any proposed solution to the proliferation of hate speech online would need to address five key issues:

- Lack of respect for diversity;
- The exponential increase in anti-social behaviour online;
- The underlying causes motivating perpetrators;

- The lack of data; and
- The lack of regulation of online service providers.

These same five issues should be addressed in the context of all harmful content found online.

I also believe any legislation intended to address harmful online content should incorporate measures relative to victims. To that end, the OFOVC has prepared a submission outlining considerations and recommendations to reflect the concerns and needs of victims.

## Considerations

### Hate speech

Available data tell us most victims of hate speech do not report it, often because they do not believe the authorities will take their complaint seriously. Reported offences are seldom prosecuted, often because the perpetrator cannot be identified. When prosecutions do take place, many cases take a long time to process, few lead to convictions, and even fewer to a custodial sentence.<sup>1</sup>

The data also tell us police-reported hate crimes targeting race or ethnicity increased substantially from 2019 to 2020 in Canada.<sup>2</sup> The Black, East or Southeast Asian, South Asian and the Indigenous populations were the targets of the majority of reported hate crimes during this period. However, we should treat these data with caution because it is unknown whether the increase is due to an increase in incidents, an increase in reporting, or a combination of the two.

While harmful online content affects everyone in unique ways, we know its effects are unequal. Thus, it is crucial the proposed legislation acknowledge vulnerable populations (e.g., Indigenous and Black persons, women, and members of the 2SLGBTQ+ community) are disproportionately affected by online harmful content. Misogynist online content is of increasing concern to OFOVC and has a disproportionate negative impact on persons who identify as women. The online community known as "incels", describing their romantic troubles - "involuntary celibacy" are almost entirely men and boys who use online forums to blame women for their sexless lives. They openly call for other incels to follow up with "acid attacks" and "mass rape." This online community praises mass killers and over the past two decades has grown with members somewhere in the tens of thousands, who have fallen under the sway of a profoundly sexist ideology that they call "the blackpill." It amounts to a fundamental rejection of women's sexual emancipation, labeling women shallow, cruel creatures who will choose only the most attractive men if given the choice. The OFOVC believes we must be prepared to confront this hateful ideology that develops online but has the potential to play out in real life, as seen in the domestic terrorist vehicle-ramming attack on April 23, 2018, in Toronto, Ontario, Canada. We recognize the intersection between this age-old misogyny and new information technologies, which can lead to everyday acts of violence ranging from harassment to violent assault.

<sup>&</sup>lt;sup>1</sup> Statistics Canada: <u>https://www150.statcan.gc.ca/n1/pub/85-002-x/2021001/article/00002-eng.htm</u> Figure 1 In only 7% of reported cases are offenders actually convicted. Only 3% serve a custodial sentence. <sup>2</sup> Ibid

Misogynistic online content or hate speech must be included in any definition regarding content that incites violence or hate speech.

It is our view that the proposed definition of hate speech in Bill C-36 is not written in plain language. Since many Canadians do not have English or French as their first language and citizens have differing levels of education, it is important for new legislation to make sense to lay persons. If people are to obey the rules, they first need to be able to understand them. This applies to those who are victims of hate speech as well: to make a complaint, they need to be able to understand what behaviour constitutes the offence. This issue should be addressed before reintroducing the Bill in the House of Commons.

## Proliferation of child sexual exploitation content and the non-consensual sharing of intimate images

According to Statistics Canada, in 2020 there were over 7,200 cybercrime-related child pornography violations, up 35% from 2019.<sup>3</sup> Statistics Canada also reported an increase of 10% in the non-consensual sharing of intimate images—sometimes known as "revenge porn"—from 2019 to 2020.<sup>4</sup> Again, it is unclear whether the increase is a true increase, an increase in reporting or a combination.

The social media industry has developed filters to screen content before uploading, thus providing an opportunity to identify images portraying child sexual exploitation and prevent it from ever reaching public view. This was the recommended approach in a 2020 report focused on the proliferation of child sexual exploitation material on the internet in the United Kingdom.<sup>5</sup>

As an example, in 2019 Facebook (includes Instagram) instituted a quarterly report "Community Standards Enforcement Report".<sup>6</sup> The report includes information about what the company is doing to protect children and data on how much content depicting child sexual exploitation they detected and removed. Facebook has reported that they detect the majority of this content before it comes to the attention of users.

However, the data cited above from Statistics Canada on reported incidents of cyber-related child sexual exploitation imply the filtering mechanisms may not be fully effective or that they are not universally applied. There may also be other channels transmitting this material.

Pre-upload screening places the burden of policing the internet squarely on the industry profiting from it. Were it fully effective, this approach could help to avoid many of the negative effects experienced by victims of child sexual exploitation and/or the publishing of intimate images without consent, simply by filtering such images out of the stream before they can be uploaded. Similarly, hate speech or content promoting or supporting terrorism would simply not appear on regular industry channels.

<sup>&</sup>lt;sup>3</sup> Statistics Canada: <u>https://www150.statcan.gc.ca/n1/pub/85-002-x/2021001/article/00013-eng.htm</u> <sup>4</sup> Ibid

<sup>&</sup>lt;sup>5</sup> The Internet: Investigation Report, March 2020: Recommendation 1, p. 102. <u>https://news-sophos.go-vip.net/wp-content/uploads/sites/2/2020/03/internet-investigation-report-march-2020.pdf</u>

<sup>&</sup>lt;sup>6</sup> Facebook: <u>https://about.fb.com/news/2021/08/community-standards-enforcement-report-q2-2021/</u>

Social media companies and law enforcement agencies should work closely together to both improve the performance of the companies in this regard and to identify and prosecute offenders.

For those concerned about the issue of freedom of expression, there are precedents in other media: newspapers do not publish material that does not conform to community standards and radio and television broadcasters can utilize technology to delay live feeds for similar purposes.

Finally, the COVID-19 pandemic has not only had an impact on Canada's economy but may also have played a role in increases in some police-reported cybercrime. Stay-at-home orders and lockdowns across the country have meant more people were at home. Children and youth were spending more time online, which increased their vulnerability to online harmful content. Authorities should make strenuous efforts to alert parents to the risks their children face online and inform them as to how to reduce those risks. Furthermore, it is of note that school staff make 90 percent of all reports of child abuse. As children have been out of school due to the pandemic, there is a risk that children may sometimes be trapped at home with the person who is exploiting them, and unable to report abuse to a trusted adult such as a teacher. My office remains concerned about the increased vulnerability of children – especially those already at risk of experiencing abuse.

## Need for training on implicit bias, cultural humility, victim-centred, and trauma-informed approaches for the proposed Digital Commissioner, Digital Recourse of Canada and the Advisory Board

Implicit bias is a mental process resulting in feelings and attitudes about people based on factors such as race, age and appearance that may influence perceptions and actions. It is an unconscious process, thus we are not aware of the negative biases we develop over the course of our lifetime.<sup>7</sup> Implicit bias supports stereotypes. It is important to understand the causes of implicit bias and intentionally work to bring it to the conscious level in order to mitigate the negative consequences. Cultural humility requires individuals to self-reflect on their own personal and cultural biases and to take note of the significant cultural realities of others.<sup>8</sup>

Using a gender-based analysis plus (GBA+) tool can help identity how different populations are affected by government policies, programs and services, taking into account intersecting identity factors (age, disability, education, language, geography, culture, income, and sexual orientation).<sup>9</sup> This type of analysis may help the proposed new regulatory bodies identify whether there are some groups that may benefit from the proposed initiatives more than others.

Since the role of the proposed Digital Safety Commissioner, Digital Recourse Council and the Advisory Board would be to oversee online content moderation, a GBA+ lens should be used as

 <sup>&</sup>lt;sup>7</sup> Workplace strategies for mental health. (2020, January 3). *Implicit Bias*. Workplace strategies for mental health. Retrieved from <a href="https://www.workplacestrategiesformentalhealth.com/resources/implicit-bias">https://www.workplacestrategiesformentalhealth.com/resources/implicit-bias</a>.
 <sup>8</sup> Yeager, K. A., & Bauer-Wu, S. (2013). Cultural humility: essential foundation for clinical researchers. *Applied nursing research : ANR*, 26(4), 251–256. <a href="https://doi.org/10.1016/j.apnr.2013.06.008">https://doi.org/10.1016/j.apnr.2013.06.008</a>

<sup>&</sup>lt;sup>9</sup> Department of Justice Canada: <u>https://women-gender-equality.canada.ca/en/gender-based-analysis-plus/what-gender-based-analysis-plus.html#about</u>

a guide. The particular needs of and barriers faced by groups disproportionately affected by harmful online content, such as people who identify as women and girls, Indigenous peoples, members of racialized communities, religious minorities, 2SLGBTQ+, gender-diverse communities and persons with disabilities should be considered.

A victim-centred, trauma-informed approach is also necessary to empower victims and survivors of online harmful content. The 2019 General Social Survey (GSS) informs us most crime goes unreported.<sup>10</sup> It is important that victims of harmful online content not only feel safe reporting their victimization, but also feel confident they will be supported afterwards. Using a trauma-informed approach will help to avoid re-traumatization, and put the focus on victims' rights, safety, well-being, expressed needs and choices, while ensuring the empathetic and sensitive delivery of services.

## The proposed mechanism to regulate harmful online content

Creating a new, separate, administrative process under the proposed new Digital Recourse Council of Canada to adjudicate complaints regarding harmful online content may not be the answer. A bureaucratic process can be both lengthy and expensive to operate, with no guarantee of efficacy.

If the Government decides to move forward with the proposed regulatory mechanism legislation in clear, plain language should be incorporated in every aspect of this approach, especially within the complaints process. The design should incorporate tools to help complainants understand whether their issue meets the established criteria for harmful online content. The purpose is not so much to screen out frivolous complaints (although it will facilitate such screening); rather, it is to enable self-screening to reduce the number of complaints not meeting the criteria. There should be consequences for filing such complaints to act as a deterrent to attempts to abuse the complaint mechanism.

While the Digital Recourse Council of Canada may be sufficient to address complaints such as hate speech, it should refer other harmful online content to the competent authorities, as is stated in the current proposal:

- If content falls within the criminal sphere (child sexual exploitation; sharing of intimate images without consent), then the criminal justice system has jurisdiction.
- If content falls within the security sphere (terrorism), then the security service has jurisdiction.

## **Complaint process**

Another important consideration of making the proposed legislation and the regulatory/ administrative regime accessible is developing a complaint process which is both easy to understand and easy to use. Canadians must be able to have confidence in the system. However, referring complaints to an administrative tribunal can make the process bureaucratic and place a heavy burden on the complainant to prove their case.

<sup>&</sup>lt;sup>10</sup> Statistics Canada: https://www150.statcan.gc.ca/n1/pub/85-002-x/2021001/article/00014-eng.htm

As an example, in 2020, the Human Rights Commission annual report indicated 49,000 people contacted the Commission to complain. The Commission accepted 1,030 complaints.<sup>11</sup> There is no hard information about how long it takes to resolve a complaint. These data imply:

- The criteria used by the Commission to screen complaints are not well understood by the general public; and
- The process is resource-intensive.

Given the performance of the Human Rights Commission in adjudicating human rights complaints, applying such a bureaucratic process to hate speech complaints may not be any more effective than the current criminal process. Additionally, this process could make it a very time-consuming and expensive mechanism.

## The potential importance of restorative justice in reconciling differences

The Government of Canada has indicated its dedication to furthering the use of restorative justice practices in Canada. Restorative justice is an alternative approach to traditional justice, with a focus on reparations and addressing the harm caused by the crime, while holding the offender accountable.

Importantly, restorative justice allows victims and survivors to play a central role in the justice process, as opposed to the traditional role of the victim as a mere witness for the state in criminal proceedings. It also allows offenders to identify and address their needs for resolution, which can help to give context to the crime and highlight areas for improvement within the community. Providing offenders with the opportunity to address the reasons for their offending behaviour and offer their perspective on the crime allows them to take responsibility for the harm done to the victim and the greater community.<sup>12</sup> This can result in psychological benefits for the victim, such as decreased fear and anxiety about re-victimization, decreased anger, increased sympathy towards the offender, and even decreased post-traumatic stress symptoms, which have positive implications for their overall well-being and ability to heal.<sup>13</sup>

Additionally, power dynamics often play an important yet undervalued role in restorative justice practices.<sup>14</sup> Variables such as age, gender, socioeconomic status or race can create explicit and implicit biases amongst the facilitators and participants, leading to a power imbalance that may be disadvantageous to one or more of the parties.<sup>15</sup> Restorative justice can be an effective tool in addressing harmful content but, ultimately, regard for power dynamics and avoiding victim re-traumatization must be at the forefront. Attention must be paid to avoid re-creating the imbalances and negative experiences seen elsewhere in the criminal justice system. It is important that experienced, trained professional mediators approach restorative justice

<sup>&</sup>lt;sup>11</sup> Canadian Human Rights Commission: <u>https://www.chrc-ccdp.gc.ca/sites/default/files/2021-04/CHRC-AR-2020-ENGLISH-WEB-FINAL.pdf p.35</u>

<sup>12</sup> Department of Justice Canada, https://www.justice.gc.ca/eng/cj-jp/rj-jr/index.html

<sup>&</sup>lt;sup>13</sup> Evans et al., (n.d.). Restorative Justice: The Experience of Victims and Survivors. Victims of Crime

Research Digest No. 11. Retrieved from <a href="https://www.justice.gc.ca/eng/rp-pr/cj-jp/victim/rd11-rr11/p5.html">https://www.justice.gc.ca/eng/rp-pr/cj-jp/victim/rd11-rr11/p5.html</a>, <sup>14</sup> Lyubansky, M. and Shpungin, E. Challenging the power dynamics in restorative justice.

<sup>15</sup> Ibid

measures delicately to avoid re-traumatization especially for some types of crime, such as child sexual exploitation and terrorist content.

#### Prevention: the best cure

The Department of Canadian Heritage's anti-racism initiative, *Building a Foundation for Change: Canada's Anti-Racism Strategy 2019–2022*,<sup>16</sup> is investing millions of dollars to combat racism and discrimination at the grassroots level via a grants and contributions program which provides funding to community organizations. According to the Departmental Plan, an evaluation of the program will take place in 2022. The results of the departmental evaluation of the program could be an important element to inform any future strategy intended to address harmful online content.

However, racism and other forms of intolerance—and their corollary—discrimination, are not local issues. While supporting the efforts of community groups is a positive step, such initiatives tend to be a localized remediation tactic rather than a general preventative strategy. I suggest a more pan-Canadian approach is necessary to address the larger issues.

A targeted educational component is an important element of a public health strategy. Focusing on emphasizing similarities between groups, encouraging acceptance of differences, and fostering critical thinking to reduce reliance on myths and stereotypes are just a few techniques to counter the effects of intolerance and discrimination.

As an example, the OFOVC has frequently pointed to the importance of providing cultural humility training for all justice system employees across the country. The training program should include elements such as:

- Raising awareness of the issues of racism, intolerance and discrimination and the harm they do;
- Focusing on cultural awareness and humility. Cultural humility is a relationship-based framework intended to address and invite equity into spaces where there has traditionally been inequity and privilege, such as the criminal justice system. Cultural humility invites those who embrace it to consider others as experts of their own lived experiences, which changes relationship dynamics to remove ego and prioritize humility. It emphasizes that we are more alike than we are different;
- Highlighting risks inherent for affected persons to make complaints about justice personnel based on:
  - Human rights violations;
  - Victims' rights violations.

#### Recommendations

#### 1. Develop clear plain language definitions of the categories of harmful content

It is essential to make the legislation and any regulatory/administrative regime accessible to all Canadians by defining the categories of harmful online content using clear, plain language and

<sup>&</sup>lt;sup>16</sup> Canadian Heritage: <u>https://www.canada.ca/en/canadian-heritage/campaigns/anti-racism-engagement/anti-racism-strategy.html</u>

and must include misogynistic online content or hate speech in any definition regarding content that incites violence or hate speech. Examples of harmful content should be included for illustrative purposes.

#### 2. Develop common terms of use for users of online services

The purpose of common terms is to describe a consistent standard of acceptable behaviour across platforms. The terms of use should be limited in number and the language should be clear. They would include users agreeing to the screening of content and acknowledging that any attempt to upload potentially illegal content would result in notification of the appropriate authority. Penalties should include temporary or permanent suspension of user privileges, depending on the seriousness of the offence. Potential users would need to read and agree to these terms before accessing the service.

#### 3. Focus on prevention: Adopt a public health approach with a strong educational component

Hate speech—and other harmful online content—are not only harmful to the direct objects of those acts. They also negatively affect our whole society, just as do infectious disease pandemics. Adopting a public health approach means focusing on prevention in addition to just response or treatment in order to reduce the number of hateful incidents and improve the overall health of society.

#### 4. Explore the options for restorative justice measures

Incorporating restorative justice practices may ultimately produce more satisfactory outcomes for victims and offenders alike.

#### Conclusion

I encourage the Government of Canada to develop new legislation from a victim-centred, trauma-informed perspective to respond to the needs of victims and survivors of harmful online content, who deserve swift action by corporations to remove harmful content from online platforms. Victims also deserve accountability when harmful content is propagated. The creation of an accompanying complaint system must be accessible and victim-centred, and the use of plain language is essential. A public health model should be instituted in addition to legislative and regulatory framework to help prevent the proliferation of harmful online content, and consideration given to the use of restorative justice measures to respond, where warranted.

From: Mark Pivon To: ICN / DCI (PCH) Subject: Open Consultation on Harmful Online Content Date: September 25, 2021 12:55:59 PM

I understand the purpose and the intent of the proposed legislative changes. And I agree that the current environment can be toxic at times - especially for marginalized persons.

#### But ...

The current proposal seems to be too broad in scope. I'm not necessarily concerned about how it might be used, now. What concerns me is how it might be twisted to serve the needs, agendas and aspirations of future political leaders. To me, it strikes me that the current proposal puts a lot of power into the government's hands to police, regulate, and ultimately control online channels. That's wrong.

When you say that the "intent is to capture major platforms", that sets off a lot of alarms. As the old saying goes "The road to hell is paved with good intentions." You can't just target "the big platforms" without also impacting the small ones. This is because once the big platforms become regulated, ALL fringe traffic will inevitably flow to the smaller ones. You would absolutely have to make the legislation sweeping and broad to have any effect. And this is too dangerous, in my view.

When you propose to censure content that might be perceived as racist, sexist, homophobic, xenophobic, or otherwise, it then opens the doors to "interpretation". This results in deliberation, evaluation, and lengthy discussion. I mean, we have PhDs in Canada who have written entire dissertations on the meaning of "The End". Imagine the deliberation on what might be construed as obscene or sexist. The cure is worse than the symptoms being targeted. AND, if deliberation is not actioned, then it's just censorship. Regardless, I'm not in favour of the government making these kinds of decisions. Sure, there are clear violations, but it is in those grey areas that concern me. Because a picture of a kid on the beach might be inappropriate in some contexts - and deserve to be vetted and moderated. But what if that picture is posted by the Leader of the Opposition? And the current government chooses to exploit that opportunity? It's not whether the image IS inappropriate, but rather the ability of someone to SUGGEST it is inappropriate citing a specific law. Once the word is out there, the damage is done. Case in point: the single tweet by Nicki Minaj suggesting a vaccine causes impotence. Social media celebrity is the real culprit and that's something the government will never be able to regulate.

It's much too dangerous because it can be used in a sense of censoring political views. It's too dangerous to be used to censure comments against corporations. It's too easy for malicious strategists to call on this sort of legislation and action strategic lawsuits against public participation. Overall, it's just too dangerous, period.

The challenge with creating laws FOR the people is that they can also be used AGAINST the people, and BY the people.

I am submitting this response to voice my opposition to the proposed changes

Regards,

Mark Pivon s.19(1) Cell:

 From:
 Doug Cloutier

 To:
 ICN / DCI (PCH)

 Subject:
 Harmful content online...

 Date:
 September 17, 2021 5:14:56 PM

This legislation is totally unnecessary. Giving the RCMP and CISIS even more oversight, when in fact their reach already is to broad. If anything we need "Less" over sight. And Canadians need more privacy laws in place to prevent this sort of unwanted privacy violating legislation..

Would expect this in China . But this I Canada or so I thought.... Sadly this will drive more people off social media and somewhere more private. As is done already in China because of over bearing laws that are infringing on our privacy.

Totally unacceptable. Canada needs more policing for white collar crimes. And less policing in general.

Doug Cloutier





September 24, 2021

Department of Canadian Heritage ("PCH")

#### Re: Google Submission to Canadian Government's Proposal to Address Online Harms

#### I. Executive Summary

We appreciate the opportunity to provide comments on the Department of Canadian Heritage's proposals to address certain categories of harmful content online. These are important issues that require thoughtful input from a variety of stakeholders, including online service providers, the Canadian government, civil society, and others.

We are supportive of the government's efforts to find ways to protect Canadians from online harms; however, we are concerned that some aspects of the current proposal could be vulnerable to abuse and may have unintended negative impacts on Canadians' access to valuable information and services, privacy and freedom of expression, and the Canadian economy. We have summarised these concerns below and provide further detail in the rest of our submission.

- The types of providers and services that are in and out of scope must be clearly identified, recognising the distinct nature of different types of services and user interactivity, differing abilities to moderate content, and the impact on access to information.
  - We agree with the government's efforts to exclude certain types of services from the definition of Online Communication Service Provider (OCSP) (e.g., private communication services, telecommunications services), and we encourage it to make these exceptions more clear to avoid creating ambiguity about the types of services it considers in scope of the proposed framework.
- Obligations must be limited to illegal content to avoid spurring the unnecessary removal of lawful, legitimate content.
  - We believe it is critical that content regulated by the proposed framework be precisely defined and limited to illegal content in order to avoid undermining access to information, limiting freedom of expression, restricting the exchange of ideas and viewpoints that are necessary in a democratic society, and creating a legal framework that could be used to censor political speech in the future. The government should take care to ensure that their proposal does not risk creating different legal standards for online and offline environments, making

## Google

legal expression offline illegal to share online. In addition, the government should avoid creating a system that drives OCSPs to adopt a "take down first, ask questions later (or never)" approach. Therefore, we urge the government to be extremely clear and precise when defining the prohibited categories and to give due consideration to the time-pressured circumstances in which OCSPs will be expected to apply these definitions to large volumes of content. Furthermore, we believe that it is essential that the government hew to existing definitions for illegal content under Canadian law in order to avoid restricting lawful expression and potentially undermining the legal validity of the framework.

 In order for illegal content to be removed expeditiously, formal legal complaint systems must be distinct from systems to address community guidelines violations. Rigid 24-hour deadlines for taking action against reported content do not allow providers to carefully assess the relevant law and context and would be counterproductive.

- 0 We agree that OCSPs should act promptly to remove illegal content when they become aware of it. However, it is critical that any legal obligations for content removal account for the nuance that is often required for these reviews and determinations, the potential for user error, the need to triage particularly egregious content, and the sheer volume of content and complaints that OCSPs need to process daily. Therefore, we urge the government to establish a flexible process for addressing illegal content that allows OCSPs to adequately evaluate removals requests within a reasonable timeframe (e.g., "without undue delay," or "expeditiously"). Moreover, any content removal legal obligations should be separate and not displace the voluntary "flagging" systems for legal, but harmful content that many OCSPs have created to address the unique needs of their products and services. We also encourage the government to clarify that OCSPs are empowered to take action against users who abuse flagging or legal notice systems and encourage the government to consider other safeguards that could be built into the framework to further deter misuse and abuse of flagging systems.
- Mandatory obligations to proactively monitor and identify content across the entire service are disproportionate and will result in the blocking of legitimate content.
  - While automated systems can be a vital tool for detecting and blocking potentially harmful content at scale, such systems often struggle with the application of nuanced, context-dependent definitions for prohibited content. Therefore, mandating that OCSPs use automated systems to proactively monitor and block content would likely lead to the blocking of large amounts of

Google

legitimate content and undermine Canadians' access to valuable information. We strongly encourage the government to clarify that the use of automated systems for proactive monitoring and blocking of content is not required and should be used in conjunction with human review. This would not preclude OCSPs from taking measures on their own initiative, where appropriate and where technologically feasible.

- Requirements to disclose user data to law enforcement agencies must be accompanied by due process safeguards to prevent the risk of unwarranted government surveillance and of encroaching on users' privacy rights.
  - We understand the legitimate needs of law enforcement, and we are supportive of OCSPs making voluntary reports to law enforcement regarding illegal content and assisting law enforcement with judicially authorized production requests. However, we are concerned that some of the proposed framework's reporting obligations may undermine due process and privacy protections, as well as directly conflict with legal obligations applicable to OCSPs in other jurisdictions. We encourage the government to reconsider the law enforcement reporting provisions and include appropriate statutory protections for privacy and due process.

 The obligation to include demographic data in regular reports to the DSC is impractical and may undermine user privacy.

- If the demographic reporting requirement were included in the framework, OCSPs would effectively be forced to start collecting additional sensitive data about Canadian users, contrary to user privacy interests and data minimization principles. It would also create an ongoing privacy risk for Canadians by forcing OCSPs to indefinitely retain detailed demographic data about all of their Canadian users, some of whom could be harmed if their sensitive demographic data were to become public as a result of a data breach. Given the significant risks associated with the mandatory collection of demographic data, we urge the government to remove the demographic data reporting obligation from the proposed framework.
- Regulatory oversight and enforcement should focus on systemic failures rather than individual cases of non-compliance so as to avoid stifling access to information, free expression, and innovation.
  - We recognize the need for appropriate sanctions for noncompliance with the law. However, we are concerned that the government's expansive enforcement powers and the open-ended nature of the framework's penalty provision will create enormous legal risk for OCSPs. For example, these provisions could

Southand contraction is a contract of Classification of the contraction of the contraction of the contract is the contract of the contract

# Google

result in OCSPs being subject to financial penalties up to 5% of global revenue for mistakes they make with respect to individual pieces of content -- even when acting in good faith and under robust compliance procedures. Given the vast amount of content that OCSPs process, the nuanced consideration that is often required to identify prohibited content, and the short deadline for addressing flagged content, it is a near certainty that OCSPs will not be able to achieve perfect compliance with the law with respect to each piece of content. These risks will effectively force OCSPs to err on the side of blocking more content than reasonably required and thereby undermine users' ability to share legitimate content and express themselves. Therefore, we urge the government to clarify and expand the due diligence defence and consider an alternative penalty framework that focuses on systemic compliance with the law.

 To avoid the unnecessary blocking or removal of lawful, legitimate content, financial and criminal penalties must be applied reasonably and proportionately.

 As discussed above, the risk of severe penalties for OCSPs that operate in good faith may pressure OCSPs into adopting imprecise and overly restrictive content moderation strategies that will deny Canadians a full opportunity to share and view legitimate content. In addition, we believe that associating penalties with an OCSP's gross global revenue results in penalties that are disconnected from the OCSP's activities in Canada and further disconnected to the reality of their potential presence in the Canadian marketplace. In order to avoid these risks, we urge the government to provide strong safeguards in the legislation that will assure that monetary penalties are imposed in a reasonable and proportionate manner.

### II. Google and YouTube's approach to content moderation

At Google, our mission is to organise the world's information and make it universally accessible and useful. We build tools to benefit society, and that have been a force for creativity, learning and access to information. They have enabled economic growth, boosted skills and opportunity, and fostered a thriving society. Google's products alone support \$1.7 billion CAD annually in incremental exports for Canadian businesses and are equivalent to 1.1% of GDP or supporting 240,000 local jobs.<sup>1</sup> In 2020, Oxford Economics found that YouTube's creative ecosystem contributed approximately \$923 million to Canada's GDP and supported more than 34, 000 Canadian jobs.<sup>2</sup> In addition, YouTube has helped Canadian creators of all kinds, both

<sup>&</sup>lt;sup>1</sup> Public First: Google Canada Economic Impact Report 2019.

<sup>&</sup>lt;sup>2</sup> Oxford Economics: From Opportunity to Impact: Assessing the Economic, Societal, and Cultural Impact of YouTube in Canada.

photheside intervention of the GAL, in the start distances (Mayor all allocies and a start intervention of the start intervention of the start of the

## Google

amateur and professional, reach a global audience. In fact, Canadian creators see 90 percent of their views come from outside Canada's borders.

While we believe the Internet has an immensely positive impact on society, we also recognise that there can be a troubling side of open platforms, and that in some cases bad actors have exploited this openness. We understand the sensitivity and importance of these areas and have devoted careful attention to developing an approach that limits harm while protecting users' ability to express themselves online. We have not waited for legislation to act in tackling illegal or lawful, but potentially harmful content; we have developed our own guidelines and taken action. We have implemented extensive efforts to help prevent and address harmful and unlawful content across our services, including by working appropriately with government, law enforcement, and other stakeholders in Canada and around the world.

Our approach for moderating content and providing our users with access to high-quality information centres on four complementary levers:

- Remove: We comply with legal obligations requiring the removal of unlawful content with clearly defined processes for users and governments to submit legal complaints about our products. In addition, we set responsible and clear rules for each of our products and services and take action against content and behaviours that infringe on them.
- Raise: We elevate high-quality content and authoritative sources where it matters most.
- Reduce: We reduce the spread of potentially harmful information where we feature or recommend content.
- **Reward**: We set a high standard of quality and reliability for publishers and content creators who would like to monetize or advertise their content.

Our strategy for tackling illegal and potentially harmful content is tailored to each of our platforms. We have processes by which governments and individuals can request removal of illegal content, including reporting violations of country-specific laws, such as those related to anti-terrorism, obscenity, or hate speech. Legal removals processes require detailed, specific information about the nature of the potentially illegal content. We review these requests closely to determine if content should be removed because it violates a law or our community guidelines and policies.

In addition, for each product, we have a specific set of rules and guidelines that are suitable for the type of platform, how it is used, and the risk of harm associated with it. For example, on

Concentration of the second se

## Google

YouTube these approaches range from clear <u>community guidelines</u>, with mechanisms to report content that violates them, to increasingly effective artificial intelligence (AI) and machine learning that can facilitate removal of harmful content before a single human user has been able to access it. In April 2021 we introduced a new metric, called <u>Violative View Rate</u>, as part of our quarterly transparency reporting. This metric estimates that the proportion of views of YouTube videos that violate our Community Guidelines has fallen from c. 0.7% in Q4 2017 to c. 0.19-21% in Q2 2021. We calculate this metric using a rigorous statistical methodology, which has just been reviewed and validated by MIT Professor Arnold Barnett.<sup>3</sup>

Our goal is to achieve both accuracy and scale in our work. That's why we have people and technology working together - and we invest heavily in both. We now have over 20,000 people across Google and YouTube dedicated to keeping our users safe from policy development to review and enforcement. This includes reviewers who work around the world across all time zones, speak many different languages, and are highly skilled. On YouTube, for example, reviewers evaluate flagged videos against all of our Community Guidelines and policies, regardless of why the video was originally flagged

While we have made tremendous progress in developing automated systems to detect harmful and illegal content, machine learning and other technologies are still in development. In some instances, automated proactive measures cannot properly take the context of content into account. Machine learning models are not yet consistently good at understanding contextual differences between content that otherwise looks very similar. As a result, automatically removing content is not necessarily the correct decision in every circumstance. In addition, recent research has also shown that even small changes to images can fool computer vision systems into missing what is obvious to human reviewers. Proactive measures are improving all the time, but they should only be deployed carefully, and when judged effective by individual companies.

We continue to invest in developing and improving the policies, products, tools, processes, and teams that handle content moderation across our platforms and are committed to providing trustworthy, useful information that meets our users needs and protects them from harm.

III. Covered Entities - The types of providers and services that are in and out of scope must be clearly identified, recognising the distinct nature of different types of services and user interactivity, differing abilities to moderate content, and the impact on access to information.

<sup>&</sup>lt;sup>3</sup> Arnold Barnett, YouTube's Violative View Rate Methodology: A Statistical Analysis (2021), available at https://storage.googleapis.com/transparencyreport/youtube/YouTube%27s%20VVR%20Methodology%2 0-%20A%20Statistical%20Assessment%20-%20Arnold%20Barnett.pdf.

Charlenand - Construction and Construction Control on Proc. Synchronic controls and Construction Construction and Sciences The Manufacture Controls on The Manufacture Controls

Google

We agree with the government's efforts to exclude certain types of services from the definition of OCSP (e.g., private communication services, telecommunications services), and we encourage it to make these exceptions more clear to avoid creating ambiguity about the scope of the proposed framework.

Because the proposed framework could require OCSPs to view and monitor certain user content, the definition of OCSP should expressly exclude services (and parts of services) where such access or monitoring is technically infeasible, would be highly intrusive to user privacy, may unreasonably limit access to high-quality information online, or harm free expression and creativity. In particular, we believe it is important that the following types of services be more clearly excluded from the definition of OCSP:

### A. Cloud storage providers

Cloud providers are limited in what they can do to address illegal content stored at the direction of their customers or their customers' users, given the technical architecture of their services, privacy protections, and the contractual obligations they hold towards their customers' data. Factually and contractually, such providers do not have the requisite authority and control over content, such that they should have responsibility for removing specific content from a third party's service. Our understanding is that the technical paper's statement that "[the OCSP definition] should not include a person who...hosts or caches the content or information about the location of the content, by reason only that another person uses their services to provide an OCS"<sup>4</sup> would prevent many cloud storage providers from qualifying as OCSPs, and we urge the government to make that point clear in legislative text.

For example, customer data may be encrypted in a manner that allows only the customer to access the data and the cloud storage provider may be contractually prohibited from accessing it. In addition, cloud services are also regularly used by government institutions, research organizations, civil society groups and universities. Placing this category of services in-scope of the definition of OCSP would require monitoring the content of such organizations. Finally, many cloud storage services, including those that directly serve consumers, generally do not make the content they store accessible or searchable to the general public. The absence of general public access and search features inherently limits the potential reach of content that is stored by cloud storage services.

Subjecting cloud services to the proposed framework would raise significant user privacy and business confidentiality concerns, among other harms. For example, the main purpose of many of these services is to allow individual consumers to store personal content. Although some users may use cloud storage services to share content with others (e.g., by sharing a link to a stored file with a limited set of other users), such sharing is often more akin to a private

<sup>&</sup>lt;sup>4</sup> Technical paper, Module 1(A), 4.

Southerstein - construction in a contribution of ACL - on Part - Signal Contribution Educational Antonio - construction of AC International Antonio - construction of AC International Contribution of ACC

## Google

communication (which are expressly exempted from the proposal) than to the widespread public distribution of content that is possible on social media services. Though some OCSPs carry out automated hash-matching of media in cloud storage, what is called for in the framework involves much more than this automated analysis. As a result, we urge the government to clarify that all cloud service providers are also excluded from the definition of OCSP. Short of that, any obligations that are placed on cloud service providers should account for the constraints on their ability to access and monitor user content.

### B. Search engines

We agree that "[the OCSP definition] should not include a person who indicates the existence or location of content,"<sup>5</sup> including search engines. Search engines play a critical role in organizing information and making it accessible to the public. They are indexes of the web at large and consist of the automatic and intermediate storage of information hosted by third parties. Given the immense volume of information that search engines process (e.g., hundreds of trillions of pages), it would be impossible for them to substantively evaluate the nature of the content they index while continuing to operate at their current scale. The content, even if it could be evaluated, would remain available on the website where it is hosted. As a result, the law has importantly ensured that responsibility rests with the platforms and webhosts that have control over the content and can determine whether it is available to the public in Canada. To ensure that search engines can continue to provide accurate and up-to-date access to the vast amount of information available on the Internet, we recommend that they continue to be expressly excluded from the definition of OCSP.

- IV. Content in Scope Obligations must be limited to clearly defined categories of illegal content to avoid spurring the unnecessary removal of lawful, legitimate content.
  - A. <u>Overbroad definitions of regulated content may limit freedom of expression and lead to over-removal of lawful content</u>

We applaud the government's overall goal of combating the spread of harmful content online. At the same time, we also believe it is critical that content regulated by the proposed framework be precisely defined and limited to illegal content in order to avoid creating a framework that spurs the over-removal of content, undermines access to information, limits freedom of expression, restricts the exchange of ideas and viewpoints that is necessary in a democratic society, and could be used to censor political speech in the future. We are concerned that the expansive and subjective content definitions proposed in the framework will make it difficult for OCSPs seeking to comply in good faith to make accurate decisions

<sup>&</sup>lt;sup>5</sup> Technical paper, Module 1(A), 4.

Constraints constraints of the constraints Constraints of the constraints of the constraints Constraints of the constraints of the constraints Constraints of the constraints of the

## Google

promptly (especially considering the proposed 24-hour deadline for addressing user-flagged content, for which we separately express additional concerns below).

For example, the technical paper states that "[t]he concept of terrorist content, should refer to content that actively encourages terrorism and which is likely to result in terrorism."<sup>6</sup> The application of this brief definition can require considerable analysis, as it requires OCSPs to consider: (1) whether the content relates to "terrorism," a term that has a fairly broad and complex definition under Canadian law; (2) whether the content is meant to "actively encourage" terrorism; and (3) whether it is "likely to result in terrorism." Faced with the pressure of having to proactively monitor vast amounts of information for prohibited content and to quickly remove and/or report prohibited content, many OCSPs will not be able to give these questions the thoughtful consideration they require. Instead, they will most likely resort to blocking/removing any content that has a remote possibility of qualifying as prohibited content that is intended to educate and inform the public about terrorism).

Consider, for example, a livestream of a political rally about climate change that is filmed by a bystander and uploaded to a social media website. While the majority of the speakers at the rally argue for activism through peaceful means, one speech raises the idea of destroying fossil fuel infrastructure in order to combat climate change. If committed, such an act could constitute "terrorist activity" under Canadian law. Therefore, an OCSP could potentially conclude that the video of speech "actively encourages terrorism" and, if the speaker is deemed to be persuasive, is "likely to result in terrorism."<sup>7</sup> Even though the bystander simply meant to raise awareness of the climate change rally and had no intention of promoting the illegal activity advocated by the one speaker, the social media site may conclude that it is required to remove the entire video and report the content and bystander to authorities. The framework also does not take into account other important considerations. For example, it does not answer the question of whether the analysis changes if the video is uploaded by a journalist. This is just one example of the proposed framework's broad definitions of prohibited content that could effectively force OCSPs to try to make nuanced decisions about the intent and impact of content at an unprecedented and infeasible scale.

Another concern is how an OCSP should handle human rights matters. For example, many individuals in Syria documented war crimes and uploaded the videos to social media sites. These videos were initially flagged by automated systems. Preserving them, however, was important for international prosecutors, human rights organizations, and Syrian citizens who

<sup>&</sup>lt;sup>6</sup> Technical paper, Module 1(A), 8.

<sup>&</sup>lt;sup>7</sup> The content could also fall into the similarly broad category of "content that incites violence," which is defined as "content that actively encourages or threatens violence and which is likely to result in violence."

aimed to hold the perpetrators accountable. Because YouTube and other social media platforms were able to retain these types of videos, they have been used as evidence in criminal cases that have resulted in convictions.

## B. Limiting the framework to categories of content that are illegal under existing Canadian law will provide clear rules and expectations for OCSPs and users

The definitions of content in scope should be directly tied to and limited to content that has been found by Canadian courts to be unlawful after a thorough review through a *Charter*-informed lens. Not doing so will likely result in legislation being found unconstitutional and will have a chilling effect on lawful expression. For example, the technical paper proposes that content related to child sexual abuse be extended to include "material relating to child sexual exploitation activities that may not constitute a criminal offence, but when posted on an OCS is still harmful to children and victims (e.g., screen shots of videos that do not include the criminal activity but refer to it obliquely; up-to-date photos of adults who were exploited/ abused as children being posted in the context of their exploitation and abuse as children)."

Most Canadians are familiar with the tragic stories of two young Canadian women who were both victims of sexualized cyberbullying and child pornography offences. After their tragic deaths, their parents bravely took on significant roles of public information and advocacy for victims, telling the stories of their daughters in order to bring about significant, positive change in our communities, our schools and in legislatures. Not surprisingly, they made extensive use of social media to reach young people with their stories of their daughters, spreading messages of respectful relationships and online safety. In one case, the victim created a video on YouTube in which she told her own story of online abuse and the impact it had on her. The definition proposed in the framework could reasonably be interpreted as requiring the removal from OCSPs of content that involves survivors and their families telling their stories for educational purposes. The definition could also be applied to OCSPs who carry public testimony from the Parliamentary committee's study that informed the framework. Ensuring that the definitions do not inadvertently silence these voices online is beneficial and completely aligned with the objective of reducing the prevalence of online material that harms children and child victims.

Given the risk of the suppression of legitimate and lawful expression, we urge the government to be precise in defining the prohibited categories of content, limit the definitions to what Canadian courts have deemed to be unlawful and to account for the fact that OCSPs will be under pressure to review enormous volumes of content and make quick determinations of whether the content falls into a prohibited category.

Madharda - analasipa - aranin 1993 - Carlor Andratan 1993 - Andrea Andrea 1993 - Andrea Andrea

## Google

As mentioned below in Section V, it is also important that illegal content has a separate legal removals system from voluntary systems OCSPs may create for their users to flag lawful content that violates their products' community guidelines. Requiring formal legal notice for removals of illegal content, would ensure that violative content is removed as expeditiously as possible. Formal legal notice would provide OCSPs with details about the illegal nature of the content as well as sufficient information about the identity and location of the individual or entity reporting the content. Additionally, OCSPs have the benefit of evaluating these illegal removals requests against clear legal standards set forth in criminal codes.

## V. Obligations for OCSPs - Rigid deadlines for taking action against reported content do not allow providers to carefully assess the relevant law and context.

We agree that OCSPs should act promptly to remove illegal content when they become aware of it. However, any legal obligations for content removal should account for the nuance that is often required for these reviews and determinations, potential for user error, and the sheer volume of content and complaints that OCSPs need to process on a daily basis. The proposed framework's 24-hour deadline for addressing all user-flagged content fails to take these realities into account and should be removed. Additionally, treating all user flags as triggers for a legal takedown obligation (including the running of the 24-hour deadline) will inevitably make the system vulnerable to abuse and lead to the removal of legitimate content.

### A. 24-hour deadline

As discussed in section IV, OCSPs may need to engage in a nuanced consideration of context, intent, and impact in order to determine whether content meets the definitions of one of the five categories of prohibited content. Given the potential breadth of the prohibited categories, "grey-area" cases will undoubtedly be common and the 24-hour deadline will not allow sufficient time for thoughtful consideration of the case (as we have noted separately, the definitions for prohibited content should also be tied to existing definitions for illegal content under Canadian law).

The problems associated with an extremely short takedown timeline will only be compounded by the fact that any user flag can trigger the start of the countdown. OCSPs that have millions of users and host billions of pieces of content could easily receive tens or hundreds of thousands of flags per day. For example, over 500 hours of video are uploaded to YouTube every minute. In the second quarter of 2021, users submitted 17,226,571 flags (around 190,000 a day) to YouTube about content that allegedly violated community guidelines. In the face of high volumes of flags, OCSPs would need to rely on automated systems for processing, which, as discussed above, struggle with making nuanced content classification decisions.

photosta construinto constitui subce construinto al attativati atta antista construinto al attativati attativati attativati attativati



In addition, confronted with the short deadline and prospect of extremely high penalties for noncompliance, many OCSPs will choose to prioritize speed over accuracy and automatically block/remove content that is subject to a flag if their automated system concludes there is even a remote possibility that the content is prohibited. As a result, significant amounts of legitimate and lawful expression that was either incorrectly flagged by a user<sup>8</sup> or mischaracterized by an automated system will be removed. While some such content could potentially be reinstated through the proposed framework's mandated appeal process, this would not eliminate the risk that Canadians would be denied access to valuable information online. Some content, for example, may be time-sensitive (e.g., news coverage of a recent event) and the removal of such content during the relevant time period would greatly undermine its value. Other content may not be appealed, in which case the legitimate and lawful expression will remain censored.

This short deadline to address takedown requests also raises considerable issues related to innovation and competition among OCSPs of differing sizes, and has the potential to stifle innovation and growth of Canadian OCSPs. Being able to address takedown requests will require personnel and other resources that are often in short supply within start ups and rapidly growing companies. While large, established companies -- particularly those that already take harmful content seriously -- will have people and processes that will have to be deployed to comply with a Canadian framework, smaller companies simply do not have these resources. This framework will immediately create a disincentive for the creation of Canadian OCSPs and overburdening the resources of smaller companies will compound the incentive to simply take down content that is at all questionable, but perhaps lawful. Furthermore, it is foreseeable that new, emerging OCSPs will simply forgo making their services available to Canadians.

It is worth noting that other democracies have avoided or pushed back against short removal deadlines for content moderation rules in recognition of the practical difficulties associated with the deadlines and their potential negative impact on consumers' right to access information and freedom of expression. For example, Germany's Network Enforcement Law (NetzDG), which includes strict content removal deadlines, only requires a 24-hour turnaround time for *"manifestly unlawful" content* and allows an extension from 24 hours to 7 days for more complex cases, as well as additional time for decisions that require specific legal expert knowledge and are referred to a joint industry body.<sup>9</sup> Similarly, in France, a 2020 bill with a 24-hour removal mandate was struck down by the French Constitutional Council over

<sup>&</sup>lt;sup>8</sup> In Q2 2021, users submitted 17,226,571 flags to YouTube, and in the same period only 351, 570 videos were removed as a result of user flags.

<sup>&</sup>lt;sup>9</sup> Network Enforcement Act (Netzdurchsetzunggesetz), Section 3.

concerns about the chilling effect the bill would have on free expression by incentivising intermediaries to remove legal speech in an effort to remain compliant.<sup>10</sup>

As an alternative to the overly brief and rigid 24-hour deadline set out in the proposed framework, we urge the government to consider more reasonable, flexible standards that would still require OCSPs to address reported content with urgency. For example, a more workable standard could be to require OCSPs to address reported content "with all due speed," "without undue delay," or "expeditiously." This would allow the company to carry out appropriate consideration and seek expert guidance, while prioritizing the most important cases. Regulators could also issue guidance or best practices that give a sense of the typical timelines in which OCSPs should generally seek to address reported content. The proposal could also include "stop-the-clock" safeguards that allow OSCPs to pause the countdown to the deadline when they require more information to evaluate the complaint.

#### B. User-submitted flags

A separate, but related problem with the obligation to address user flags within 24 hours is the fact that user-submitted flags are often inaccurate and can be used as a tool to harass and infringe on the expression of other users. Our experience with the YouTube community guidelines flagging tool illustrates this risk. We receive hundreds of thousands of content flags on a daily basis. While many are good-faith attempts to flag problematic content, large numbers of them represent mere disagreement with views expressed in legitimate content or are inaccurate. These types of user flags are best used as "signals" of potentially policy violative content, rather than definitive statements of violations, and should not be treated as flags that trigger specific legal obligations. It is critical that OCSPs have discretion to review and use such flags in ways that make the most sense to protect their users (e.g., evaluating flags in conjunction with technical signals and other factors to prioritize reviews of flagged content).

Our experience with Germany's NetzDG law provides similar evidence about the inaccuracy of user flags even in the context of a legal complaint system. Our current NetzDG transparency report shows that more than 84% of content reported under the NetzDG was determined not to violate our Community Guidelines or the criminal statutes referred to in NetzDG and was therefore not removed or blocked.<sup>11</sup>

https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm.

" Removals under the Network Enforcement Law, available at:

<sup>&</sup>lt;sup>10</sup> Decision n° 2020-801 DC of June 18, 2020, available at

https://transparencyreport.google.com/netzdg/youtube?hl=en.

Marković, osobovejo co osta 1933. u Secolar, articatikaj 1960. grafitako co ostali post 170. statu 1971.

## Google

Given the high risk of inaccurate user flags, we urge the government to consider alternative approaches, such as requiring users to submit a legal complaint. If users were to submit such a complaint, they would be required to provide the legal grounds for the removal, their identification, and precise location. This standard has been successfully implemented in regulations across the globe, including most recently in France. Adding more specificity to the user reporting process would not only increase the likelihood that users will report actionable content but also provide us with the information we need to evaluate the content fairly and quickly.

We encourage the government to consider permitting OCSPs to require that users provide detailed information about the nature of their report-- if they are claiming that the content is prohibited under Canadian law. For example, a formal report pursuant to the Canadian framework should require the user to:

- identify themselves;
- clearly identify the content at issue by URL, video timestamp, or other unique identifier.
- state the law and basis of the legal claim (e.g., explain why the content meets the definition of one of the prohibited categories of content); and
- attest to the good faith and validity of the claim.

The government and OCSPs could collaborate to provide guidance and educational resources in order to help users understand the nature of the law and complete these requests. However, we believe that it is important to maintain a distinction between complaints that trigger significant legal requirements and the simple 'click to flag' buttons that are used for community guideline violations that may not have legal implications. Requiring users to go through additional steps to submit a legal complaint would highlight the significance of the action and potentially deter abuse of the system. Reducing the number of incorrect or abusive complaints submitted pursuant to the legal reporting requirement will also enable OCSPs to spend more time on legitimate complaints and help them block prohibited content in a timely manner.

Alternatively, notice could be limited to removal requests submitted by certain trusted organizations. For example, YouTube has developed a Trusted Flagger program to help provide robust tools for individuals, government agencies, and non-governmental organizations (NGOs) that are particularly effective at notifying YouTube of content that violates our Community Guidelines. The program provides these partners with training, a bulk-flagging tool, and a channel for ongoing discussion and feedback about YouTube's approach to various content areas. The program is part of a network of more than 180 academics, government partners, and NGOs that bring valuable expertise to our enforcement systems. For instance, to help address violent extremism, these partners include the International Centre for the Study of Radicalization at King's College London, the Institute for Strategic Dialogue, the Centre for Israel and Jewish Affairs, the National Council for Canadian Muslims and government agencies

onorbierte construction construccales en la cara anna anna an desegnations construction qui son transmission construction

## Google

focused on counterterrorism. Because their flags have a higher action rate than the average user, we prioritize them for review.

Lastly, we encourage the government to clarify that OCSPs are empowered to take action against users who abuse flagging or legal notice systems. For example, under flagging systems that platforms have voluntarily established, platforms have the ability to ban users who repeatedly make false reports. The framework should provide OCSPs with a safe harbour from liability for actions they take to ban or otherwise penalize users who misuse any legally mandated flagging system. In addition, we encourage the government to consider other safeguards that could be built into the framework in order to further deter misuse and abuse of flagging systems.

#### VI. Obligations for OCSPs - Mandatory obligations to proactively monitor and identify content across the entire service are disproportionate and could result in the blocking of legitimate content.

We are supportive of OCSPs voluntarily implementing robust systems to identify and address harmful content. We are concerned, however, about the potential negative consequences of the proposed framework's broad requirement that OCSPs "take all reasonable measures, which can include the use of automated systems, to identify harmful content that is communicated on its OCS and that is accessible to persons in Canada, and to make that harmful content inaccessible to persons in Canada."12 Specifically, we are concerned that some could seek to interpret this language as a mandatory obligation to implement automated systems that proactively monitor and block prohibited content. As discussed in more detail below, doing so would create a series of significant negative ripple effects for Canadian users. For example, given that it is often difficult for automated systems to determine whether content falls into highly context-dependent categories (e.g., the five prohibited categories of content under the framework), the required use of such systems would likely result in the over-blocking of content and Canadians losing access to valuable content and information. Additionally, bad actors may seek to exploit weaknesses in these automated systems in order to intentionally censor legitimate content (e.g., political speech, speech by minority groups). To avoid these negative outcomes, we encourage the government to clarify that no part of the framework mandates the proactive monitoring and filtering of content.

While breakthroughs in machine learning and other technology used to monitor and identify potentially harmful content are impressive, the technology is still evolving and is less accurate for more nuanced or context-dependent content. For example, automated systems that are trained to recognize certain images or patterns of text that may be associated with categories of prohibited content (e.g., terrorist content, hate speech) may mistake news coverage,

<sup>&</sup>lt;sup>12</sup> Technical paper, Module 1(B), 10.

500

## documentaries, educational material, and academic research of these subjects as prohibited content because they contain some of the same images and text.

Consider a video of military conflict. In one context, the footage might be documentary evidence of atrocities in areas that journalists have great difficulty accessing. In another context, the footage could be promotional material for an illegal organisation (e.g., a terrorist organisation). And in another, important political speech by marginalized populations. In the same vein, the exact same iconic and horrifying images of historic genocide are used by those who want to advocate for justice and tolerance, on one hand, and those who advocate for violence and further genocide, on the other hand. Between these two poles are those who aspire to report on historic events in an objective manner. Computers cannot yet distinguish this key context. Even a highly trained reviewer could have a hard time telling the difference, and machines are even more limited.

Similarly, while automated systems can make it easier to prevent known violative content from being re-uploaded, they have limitations here as well. For example, on YouTube, we use digital hash technology to catch copies of known violative content before it is available to view. For some content, like child sexual abuse images and terrorist recruitment videos, we contribute to shared industry databases of hashes to increase the volume of content our machines can catch at upload. This technology generally works well when *exact* copies of, for example, the same terrorist propaganda video are re-uploaded. In contrast, an automated tool may have difficulty detecting the same video if it has been subject to minor alterations.

The accuracy limitations of automated systems can also be seen in data we maintain about appeals on YouTube. From April-June 2021, we received 217,446 requests for appeal, an increase from the previous quarter; of those, 52,696 videos were reinstated.<sup>13</sup> During the onset of the COVID-19 outbreak, there was an increase in successful appeals which may have been attributable to an increased deployment of machine learning to tackle challenging content during that period, and thus reinforces the view that machine automation simply cannot replace human judgment which requires time for proper analysis and deliberation.

In addition to potentially blocking legitimate speech, mandatory proactive monitoring requirements may also stifle innovation and competition in the OCS industry in Canada. Building and implementing automated systems to monitor content can entail substantial costs and engineering, legal, and trust and safety resources. Small companies and startups may be deterred from entering the OCS market in Canada if they are unable to bear these costs.

<sup>&</sup>lt;sup>13</sup> Google Transparency Report, available at:

https://transparencyreport.google.com/youtube-policy/appeals?hl=en&total\_removed\_videos=period:20 20Q1;exclude\_automated:all&lu=total\_videos\_reinstated&total\_videos\_reinstated=period:2019Q4.

 Southerster, construction and control to a definition description and controls of Champion and a construction and a definition of the control of the contro

## Google

Given the limitations of automated systems and risks associated with their use, several other countries and organizations have taken a strong stance against general content monitoring obligations. For example, the EU's e-Commerce Directive<sup>14</sup> and proposed Digital Services Act<sup>15</sup> contain express prohibitions on mandating "general monitoring." The EU Commission stated that requiring monitoring "could disproportionately limit users' freedom of expression and freedom to receive information, and could burden service providers excessively and thus unduly interfere with their freedom to conduct a business. The prohibition also limits incentives for online surveillance and has positive implications for the protection of personal data and privacy."16 A 2018 UN report on freedom of expression also stated that "[s]tates and intergovernmental organisations should refrain from establishing laws or arrangements that would require the 'proactive' monitoring or filtering of content, which is both inconsistent with the right to privacy and likely to amount to pre-publication censorship."<sup>17</sup> Similarly, several organisations dedicated to promoting and protecting fundamental rights and freedoms in the digital environment have stated that "general monitoring would undermine free expression and privacy by imposing ongoing and indiscriminate control of online content with mandatory use of technical filtering tools."18

We urge the government to clarify that the "reasonable measures" that are required by Module 1(B) of the proposal do not include mandatory proactive monitoring and filtering of content. Such a clarification would help avoid the problems discussed above and better align the framework with international norms.

VII. Notification to Law Enforcement - Requirements to disclose user data to law enforcement agencies must be accompanied by due process safeguards to prevent the risk of unwarranted government surveillance and of encroaching on users' privacy rights.

<sup>&</sup>lt;sup>14</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Article 15.

<sup>&</sup>lt;sup>15</sup> Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, Article 7.

<sup>&</sup>lt;sup>16</sup> Proposal for a Regulation of the European Parliament and the Council on a on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0825&rid=2,

<sup>&</sup>lt;sup>17</sup> "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," United Nations (2018), available at

https://ap.ohchr.org/documents/dpage\_e.aspx?si=A/HRC/38/35.

<sup>&</sup>lt;sup>18</sup> Letter to Members of the Telecommunications Council, Executive Vice-President Vestager, and Commissioner Breton (June 4, 2020), available at

https://cdt.org/wp-content/uploads/2020/06/Telecommunications-Council-Joint-Letter.pdf.

We are supportive of OCSPs making voluntary reports to law enforcement regarding illegal content and assisting law enforcement with judicially authorized production requests;<sup>19</sup> however, we are concerned that some of the proposed framework's reporting obligations may undermine due process and privacy protections and conflict with OCSPs' other legal obligations.

Google

The general reporting provisions in the proposed framework would require OCSPs to:

- notify the RCMP in circumstances where the OCSP has reasonable grounds to suspect that content falling within the five (5) categories of regulated harmful content reflects an imminent risk of serious harm to any person or to property, as may be prescribed through regulations established by the Governor in Council; or
- [as an alternative] report prescribed information in respect of prescribed criminal
  offences falling within the five (5) categories of regulated harmful content to
  prescribed law enforcement officers or agencies, as may be prescribed through
  regulations established by the Governor in Council. Under this provision, OCSPs would
  also be required to report information respecting terrorist content and content that
  incites violence that will be made inaccessible in accordance with this legislation to the
  Canadian Security Intelligence Service (CSIS) in a manner that conforms to Governor in
  Council regulations relating to the threshold, timing, format and any other requirements
  for such reports.<sup>20</sup>

Both of these proposed approaches notably do not call for this data sharing process to be overseen by an independent judicial authority, as is required to comply with Section 8 of the *Charter*: Canadian courts have held that law enforcement must have a court-approved production order to obtain such user data from OCSPs. Additionally, the proposal gives the Governor in Council discretion to specify the information that must be included in the notifications or reports.<sup>21</sup>

Absent further clarification in the legislation, we are concerned that these provisions may require OCSPs to regularly provide extensive amounts of user data to law enforcement authorities. Given the breadth of the definitions for the five categories of prohibited content and risk of heavy penalties for noncompliance, many OCSPs may feel pressured to report any content that could *potentially* fall into the prohibited categories. In addition to flooding law enforcement entities with many unhelpful reports about non-prohibited content, this regular

<sup>&</sup>lt;sup>19</sup> Google receives law enforcement requests for data from all over the world, and we have a dedicated team that responds to them around the clock, every day of the year. We also work to streamline the process for governments to obtain digital evidence. For example, our Law Enforcement Request System (LERS) allows a verified law enforcement agent to securely submit a legal request for user data, view the status of the submitted request, and download the response submitted by Google.

<sup>&</sup>lt;sup>20</sup> Technical paper, Module 1(B), 20.

<sup>&</sup>lt;sup>21</sup> Technical paper, Module 1(B), 20.

Southerstein consistency on the contribution of the set Part - Syndry and installer to be considered as the contribution of the the second as the second set of the second to the second set of the second second

## Google

flow of large volumes of user data from private companies to law enforcement organizations without user knowledge would violate consumer expectations about privacy and government surveillance in a democratic country. The establishment of such a reporting system may also restrict political speech and free expression, as users may be hesitant to publish legitimate content that relates to prohibited content (e.g., a documentary about terrorism) if they know that it may lead to their information being reported to law enforcement.

While it is possible that some of the privacy impacts of the reporting obligations could be mitigated by limiting the contents of the law enforcement report to information about the content itself (which will in some cases be publicly available), serious privacy risks would remain. For example, many OCSPs provide users with the ability to limit the audience of content they post. In cases where a user has shared content with a handful of people, the content is arguably more akin to a private communication than publicly available information. Private communications are expressly exempted from the framework, and we encourage the government to ensure that similar communications are given similar treatment under the framework.

The Supreme Court of Canada has observed that anonymity is one of the key elements of constitutionally-protected privacy, and this is "particularly important in the context of Internet usage.<sup>22</sup> The provision of identifying information to law enforcement could also potentially affect the user's *Charter* section 8 rights related to unreasonable search and seizure. Currently, Canadian law enforcement agencies are only able to obtain information about an Internet user who has posted content online if they prove to a judge, under oath, that "there are reasonable grounds to believe that an offence has been or will be committed under this or any other Act of Parliament". The judge is then tasked with determining whether the public interest in the police acquiring this information outweighs the privacy and other public interests at stake. The proposed framework for notification to law enforcement removes this judicial check, which has been developed in order to balance the critical constitutionally protected interests at stake. In essence, it replaces a cornerstone of our legal system, the impartial judge, with a private sector entity that has been structurally incentivised to over-report.

The reporting obligations may also conflict directly with legal obligations applicable to OCSPs in other jurisdictions. For example, the personal data of users/customers in the European Economic Area (EEA) and Switzerland is subject to the protections of the EU's General Data Protection Regulation (GDPR). If an EU data subject posts content that triggers the law enforcement reporting requirements, an OCSP that is subject to the GDPR may be unable to share the personal data of that user with Canadian law enforcement organizations due to the limitation of Canada's adequacy decision to commercial organizations. The disclosure would either be simply unlawful or may risk violating the applicable EU laws. Such a dilemma would

<sup>&</sup>lt;sup>22</sup> R. v. Spencer, 2014 SCC 43, at para 45 <<u>https://canlii.ca/t/g7dzn#par45</u>>.

nog konstruction for general and the set of the stand of the statement Robinski for the statement of the for sector of the Mandata Mandata State

## Google

force the OCSP to choose between the risk of significant penalties for noncompliance with the proposed framework and the risk of significant fines for violations of the GDPR if an OCSP were to disclose the personal data of European users. It may also risk substantial damages payable to the affected individual, as a mandatory disclosure in Canada would not be a defence to a claim in the EEA. It is well established within customary international law and Canadian domestic law that a legal requirement in Canada that would cause an offence under another country's law offends sovereignty, comity and international norms. The Canadian framework for online harms needs to take this into account, particularly where the other jurisdiction is closely allied with Canada.

Given the risks associated with the current reporting requirements, we urge the government to include appropriate statutory protections for privacy and due process. Potential revisions could include narrowing the scope of the reporting requirements and/or prescribing the specific information that must be included in a report instead of leaving that issue to the discretion of the Governor in Council.

#### VIII. Reports to the Digital Safety Commissioner - The obligation to include demographic data in regular reports to the DSC is impractical and may undermine user privacy.

While we agree that it is important for the government to examine the impact of online harms on different demographic populations, we believe that the mandated inclusion of demographic data in OCSP reports to the DSC is unlikely to yield accurate or helpful information and may undermine user privacy by forcing OCSPs to collect sensitive demographic data when it is otherwise not necessary. Currently, the proposed framework provides that OCSPs must generate and provide reports on a scheduled basis to the DSC on Canada-specific data that includes, among other things, "information on their (a) notifications to the Royal Canadian Mounted Policy (RCMP) or (b) reporting to law enforcement" and, for such notifications, "anonymized and disaggregated information about the kinds of demographics implicated."<sup>23</sup>

Many platforms would simply be unable to comply with this requirement under their current data collection practices. OCSPs often do not collect detailed demographic data about their users because: (a) it is frequently not necessary in order to provide services to users; and (b) such data can be sensitive personal information and is subject to additional legal protections in many jurisdictions around the world, including Canada. For example, Canadian privacy laws follow the "data minimisation principle" and require organizations to only collect personal information where it is reasonably necessary to perform the services being delivered. Therefore, if the demographic reporting requirement is included in the framework, OCSPs would effectively be forced to start collecting this sensitive data about Canadian users. Forced

<sup>23</sup> Technical paper, Module 1(B), 14.

collection of this data runs contrary to user privacy interests and conflicts with general norms regarding data minimization. It would also create an ongoing privacy risk for Canadians by forcing OCSPs to indefinitely retain detailed demographic data about all of their Canadian users, some of whom could be harmed if their sensitive demographic data were to become public as a result of a data breach.

It is also important to note that this blanket collection of demographic data may yield inaccurate information. For most OCSPs, the only practical way to collect demographic data will be through user self-reporting. Where users are forced to provide this data, they may choose to report inaccurate data in order to protect their privacy or signal their resistance to this unwanted mandate. Additionally, if it becomes widely known that the government relies on this data in order to understand the impact of online harms on different demographic populations, bad actors may intentionally report false demographic data in an attempt to undermine this goal (e.g., a malicious user may self-report membership in a marginalized group before posting hate speech about that group).

Given the significant risks associated with the mandatory collection of demographic data, we urge the government to remove the demographic data reporting obligation from the proposed framework.

- IX. A New Regulatory Scheme Regulatory oversight and enforcement should focus on systemic failures rather than individual cases of non-compliance so as to avoid stifling free expression and innovation.
  - A. Focus on systemic noncompliance

We recognize the need for appropriate sanctions for noncompliance with the law. However, we are concerned that the expansive powers granted to the Digital Safety Commission and the open-ended nature of the proposed framework's penalty provision will result in OCSPs being subject to significant financial penalties for mistakes they make with respect to individual pieces of content, even when acting in good faith and under robust compliance procedures. This will have negative consequences for freedom of expression and innovation in the OCS industry.

Under the current proposal, the Digital Safety Commissioner is given the power to "require an OCSP to do any act or thing, or refrain from doing anything necessary to ensure compliance with any obligations imposed on the OCSP by or under the Act."<sup>24</sup> Additionally, it provides that administrative monetary penalties may be imposed on an OCSP for failure to comply with such

05009.07907/01/01/02/02/02/03/07/07/07

200ale

<sup>24</sup> Technical paper, Module 1(D), 80.

an order, or for "[a]ny other violations of the Act or regulations."<sup>25</sup> Given the vast amount of content that OCSPs process, the nuanced consideration that is often required to identify prohibited content, and the short amount of time that OCSPs have to evaluate flagged content, it is a near certainty that OCSPs will not be able to achieve perfect compliance with the law with respect to each piece of content.

Google

Therefore, it is possible that an OCSP that has acted in good faith and implemented robust procedures to comply with the law could nonetheless be subject to a significant penalty if, for example, it fails to report certain prohibited content to law enforcement because of an oversight by its automated systems. OCSPs that act in good faith could also be held liable for failure to adhere to inaccessibility orders.<sup>26</sup> For example, an OCSP that takes all reasonable steps to comply with an order to block content could fail to comply with its obligations if a user uploads a slightly altered version of the prohibited content that evades the OCSP's automated systems.

These risks will effectively force OCSPs to err on the side of blocking more content than reasonably required (e.g., adjusting their automated systems so they are overly sensitive in detecting content that *may* be prohibited) and thereby undermine users' ability to share legitimate content and express themselves. It may also stifle innovation and deter new entrants in the OCS space, as the cost of providing such services will incorporate a high risk of significant regulatory penalties.

Although the framework does include a due diligence defence<sup>27</sup> that could potentially prevent a good faith OCSP from being subject to penalties, the scope and requirements to qualify for that defence are currently unclear. The common law due diligence defence has generally been developed and refined in connection with strict liability regulatory offences (such as pollution and motor vehicle offences) that are very different from the present context, which inherently requires the exercise of judgement and investigations into the context in which content was created or posted. The framework should articulate a defence of due diligence that takes account of the complexity of interpreting expression and anticipating harm within an enormous quantity of material. Additionally, the OCSP would still bear the cost of defending itself in a proceeding and raising that defence.

In order to avoid these negative outcomes, we urge the government to clarify and expand the due diligence defence and consider an alternative penalty framework that focuses on systemic compliance with the law. A framework centred around systemic compliance would allow the government to go after wilful noncompliance and the worst offenders while avoiding

<sup>&</sup>lt;sup>25</sup> Technical paper, Module 1(D), 94.

<sup>26</sup> ld.

<sup>&</sup>lt;sup>27</sup> Technical paper, Module 1(D), 110.

Machards, construction construcistas, a decisivati anticatation Machards attaction construction Machards attaction construction Machards attaction

# Google

the creation of perverse incentives that force good-faith OCSPs to adopt overly restrictive content moderation systems that harm consumers and society. For example, transparency requirements in the law can provide regulators with a window into the complaints that the OCSP receives and the processes it has in place to address prohibited content. Where systematic failures are suspected, the regulator can conduct a more thorough investigation and impose penalties as appropriate (e.g., "naming and shaming" the OCSP for its failure to meet its obligations, imposing monetary penalties).

The majority of OCSPs will endeavour to comply with all their legal obligations related to content in scope and will act in good faith in doing so. However, both machines and humans are fallible, particularly when it comes to the inherently subjective exercise of parsing content that requires context in order to determine whether it fits into the five categories of online harms. There will also be a "learning curve" as new requirements are implemented and disseminated through an organization. Any resulting framework should recognize this and require that the regulators first take a remedial approach when dealing with individual complaints and systemic issues that are appropriately addressed through collaboration and cooperation with the regulators.

Under this approach, it will be particularly important for the regulations to clearly describe what constitutes a "systemic failure" in order to provide OCSPs with clarity about their obligations. This definition should consider factors such as the amount of content processed by the OCSP, the amount of prohibited content identified on the OCS, and the success rate in promptly addressing prohibited content.

#### B. Blocking of content by telecommunications service providers

Another aspect of regulatory power provided under the framework about which we have concern is the Digital Safety Commissioner's power to apply to the Federal Court to seek an order to require Telecommunications Service Providers to implement a blocking or filtering mechanism to prevent access to all or part of a non-compliant OCSP's service in Canada, where that OCSP has repeatedly refused to remove child sexual exploitation and/or terrorist content.

While we agree in principle with the application of this proposal to child sexual exploitation content, its application to terrorist content, which is much more context-dependent, requires carefully crafting the definition of "terrorist content" to ensure that the government cannot use such language to stifle expression that the government does not agree with. It is a slippery slope from this type of blocking for context-dependent content to state-sanctioned Internet censorship, which could have serious consequences for Canadian citizens' freedom of expression and access to information.





#### X. Incident Response Protocol

We recognize the importance of implementing the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online. In May 2019, Google and YouTube signed the Christchurch Call to Action. As part of our steps to implement the Call, the Global Internet Forum to Counter Terrorism (GIFCT), of which YouTube is a founding member, developed the Content Incident Protocol (CIP) for industry to respond efficiently to perpetrator-created content after a violent attack. The CIP is a process by which GIFCT member companies quickly become aware of, assess and address potential content circulating online resulting from an offline terrorist or violent extremist event. The CIP sits alongside, and is complementary to, national and multinational crisis response protocols.

Since the attack in Christchurch, GIFCT member companies have developed, refined and tested the CIP through workshops with Europol and the New Zealand Government. To date, we have activated the protocol twice; after the attack on a synagogue in Halle, Germany in October 2019 and following a shooting in Glendale, Arizona in May 2020. In addition, GIFCT members have mechanisms to exchange situational awareness which, since April 2019, we've used over 150 times following terrorist or violent extremist attacks around the world.

The proposed framework allows the DSC to establish a national incident response protocol.<sup>28</sup> We urge the government to ensure that any such national protocol be consistent with the CIP. As noted above, the CIP represents a globally-coordinated approach to implement the Christchurch Call to Action. The introduction of a national approach inconsistent with the CIP risks undermining the effectiveness of the latter, particularly in time-critical situations, as OCSPs would be forced to grapple with multiple competing frameworks.

#### XI. Penalties - To avoid the unnecessary blocking or removal of lawful, legitimate content, financial and criminal penalties must be applied proportionately.

As discussed above, we are concerned that that proposed framework will create a system that unduly punishes OCSPs that operate in good faith and, as a result, pressures OCSPs into adopting imprecise and overly restrictive content moderation compliance strategies that will deny Canadians a full opportunity to share and view legitimate content. These risks are greatly exacerbated by the size of the penalties that are permissible under the proposed framework.

As drafted, the framework allows for penalties of up to the higher of \$25,000,000 or 5% of the OCSP's gross global revenue.<sup>29</sup> Such figures create enormous legal risk for OCSPs, particularly

<sup>&</sup>lt;sup>28</sup> Technical paper, Module 1(B), 18.

<sup>&</sup>lt;sup>29</sup> Technical paper, Module 1(D), 119.

if violations can be imposed for noncompliance with respect to individual pieces of content. The threat of these fines may deter established companies from providing OCS services in Canada and discourage startups in the OCS space from launching in Canada.

The range of penalties set out in the framework is disproportionate to the underlying actions sought to be deterred. Associating the penalties with an OCSP's gross global revenue results in penalties that are disconnected from the OCSP's activities in Canada and further disconnected to the reality of their potential presence in the Canadian marketplace. While the factors to be considered in the imposition of any particular penalty will hopefully be connected to the blameworthiness of the conduct, its recklessness and the harm that may have arisen with respect to Canadian residents, pegging penalties to global turnover unnecessarily but inevitably focuses on a company's operations that are wholly disconnected from Canada, and thus from any regulatory impact in Canada.

In addition, the possible imposition of penalties related to the blocking of content that has not been determined by a court of competent jurisdiction to actually be unlawful penalizes OCSPs whose only malfeasance is failing to block access to content that a complainant and a regulator consider to be likely unlawful in Canada.

In order to avoid these risks to free expression and innovation, we urge the government to provide strong safeguards in the legislation that will assure that monetary penalties are imposed in a reasonable and proportionate manner. Although the current text of the framework lists factors that must be considered when determining the amount of a monetary penalty,<sup>30</sup> a clear requirement for proportionality and greater guidance on the application of these factors are needed. Such steps would help the framework better align with international norms regarding content moderation laws.<sup>31</sup>

Thank you for the opportunity to comment on Canada's proposed approach to address harmful content online. We are committed to continuing our efforts to ensure our platforms provide a safe community where our users can thrive and we welcome the opportunity to discuss our recommendations in more detail.

<sup>&</sup>lt;sup>30</sup> Technical paper, Module 1(D), 107.

<sup>&</sup>lt;sup>31</sup> See, e.g., "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," United Nations (2018) (discouraging states from "imposing disproportionate sanctions, whether heavy fines or imprisonment, on Internet intermediaries, given their significant chilling effect on freedom of expression.").

Document communiqué en vertu de la Loi sur l'accès à l'information Document released pursuant lo line Access la Information Act.



## National Association of Friendship Centres

Association nationale des centres d'amitié



# **NAFC Comments**

## **Regulating Harmful Online Content**

September 2021

Submitted by: Gabriel Maracle, Policy Analyst (gmaracle@nafc.ca) On behalf of the National Association of Friendship Centres

275 MacLaren Street Ottawa, Ontario K2P oL9 (613) 563-4844



Decument communities en ventu de la Lei sur l'acola à l'intermetion Obcument released pursuant to the Acores la information Act.

NAFC.ca

Searchansar - conservingent et is contra a - El Certo Paris Sy El Carlo antenno - Desconadores - contra a en el - Desconadores - Cherri - Desc

## **Overall comments:**

The National Association of Friendship Centres (NAFC) is the national body of the Friendship Centre Movement (FCM). The NAFC represents over 100 Friendship Centres and Provincial/Territorial Associations (PTAs) from coast to coast to coast. The NAFC and its members provide supports for urban Indigenous people across Canada. Addressing harmful online content that can potentially make social media platforms safe spaces for urban Indigenous people is essential to the NAFC and the broader FCM. A great deal of the FCM's communication strategies is through social media and online platforms. A study of health access of Indigenous youth highlighted that a significant source of information for youth is a mixture from community, Friendship Centres, and the internet. Protecting Indigenous and other marginalized communities online from harmful content is a critical mission. However, there are several questions and concerns that the NAFC has about the proposed new sets of legislation. The primary concern is the implementation of oversights of both approaches proposed. There needs to be active participation of urban Indigenous voices in both of these processes. The Federal Government has framed regulating harmful online content to protect those vulnerable and marginalized, including urban Indigenous peoples. This submission has been divided into two sections to address both proposed models.

## Module 1: New Legislative and regulatory framework

Having the voices and perspectives of Indigenous people in the moderation of online content should be a part of the advisory board. Given that the legislation would include establishing an advisory board for the Digital Safety Commissioner and the Recourse council, there should be adequate representation from urban Indigenous people as social media and the internet are potent platforms as digital communal spaces for Indigenous peoples.

The inclusion of Indigenous voices in all levels of the Digital Safety Commission is vital to reflect the values and perspectives that the Commission seeks to protect. An advisory council comprised of various voices and perspectives can provide advice and guidance to the Commissioner (DSCC) and the Recourse Council (DRCC). However, how the DSCC and the DRCC will interact with the advisory board is unclear; more information is needed about how the advisory board will be staffed and navigate this relationship.

There is also the issue that much harmful online content does not live on common mainstream social media platforms. Online Canadian hate groups have flourished over the past few years, many of which are not mainstream social media platforms. Many mainstream social media platforms have tried to address harmful online content with mixed results. Although some prominent far-right figures have been de-platformed from most mainstream social media sites, de-platforming extremist figures and content disrupts dissemination; it does not eliminate it. An ecosystem of alternative media and platforms, such as Gab, Parler, Telegram, or 8kun, allows harmful online content on its platform through lax or non-existent content moderation. Many of these platforms are anonymous or use VPNs to encrypt their data or are communities on the Deep Web and Dark Web. There does not appear to be any components of the legislation that address content on encrypted platforms.

### Module 2: Modifying Canada's existing legal framework

The NSIRA should include urban Indigenous representation to ensure that checks and balances are maintained and that urban voices are heard when CSIS deals with potentially harmful online content.

Modifying Canada's current legal framework also raises questions and concerns. The NAFC has concerns about modifying the CSIS act. When expanding the CSIS act, there is mention of allowing CSIS to have a new jurisdictional authorization to obtain either transmission data or basic subscribe information for the sake of national security. There is no information on how CSIS would determine what constitutes a national threat; it is an ambiguous process that could easily lead to abuses.

Indigenous-led organizing, community, and resistance have flourished online with the Red Dress Day or the Idle No More Movement. Any time there is some form of national action, protest, or resistance, Indigenous people on social media have to bear the brunt of inflammatory, racist and hateful comments, posts and videos. Through demonstrations and occupations, Indigenous resistance to resource extraction and development rely on social media as a significant part of their communication strategy. These acts of resistance could easily be framed as anti-government or manifestations of Indigenous cyber—terrorism, which are genuine concerns held by government agencies around the globe. There is a legitimate risk of governing bodies weaponizing this legislation to identify protests as antigovernment, especially when Indigenous people across Turtle Island articulate their inherent rights and sovereignty.

The historical oppression of Indigenous actions should not be ignored, particularly concerning the efforts of national intelligence organizations. Modifying the CSIS act to address harmful online content and threats to national security should also ensure the inclusion of the National Security and Intelligence Review Agency (NSIRA) in this process. Having oversight in protecting communities from harmful online content ensures that marginalized communities are not harassed by those that claim to protect them.

Nacument communique en verto de la Lei sur l'accès à l'information riscument rerences pursuant lo me licoess la manmateri Aci-



## Canada

September 2021

Submission to the Consultation on the Government of Canada's Proposals to Address Harmful Content Online

Centre for Law and Democracy info@law-democracy.org +1 902 431-3688 www.law-democracy.org fb.com/CentreForLawAndDemocracy @Law\_Democracy

## Table of Contents

1. In	troduction1
2. A	pplicable Legal Framework and Relevant Human Rights
2.1.	Freedom of Expression
2.2.	Privacy
2.3.	The Rights of Others
3. T	he Definitions of Harmful Content
3.1.	
3.2.	Hate Speech
4. W	Tho and What Will be Regulated
5. Fa	our New Regulatory Bodies
6. T	he User-flagged Content Moderation System
6.1.	The Proposed User-flagged Content Moderation System
6.2.	Assessment of the User-Flagged Content Moderation System
6.3.	Caseload of the Digital Recourse Council of Canada15
7. 0	CSPs Proactive Obligations
7.1. Inac	OCSPs to Take "All Reasonable Measures" to Identify and Make Harmful Content cessible
7.2. Serv	OCSPs to Have New Reporting Obligations to Law Enforcement and Intelligence ices
8. W	lebsite Blocking
Recom	mendations

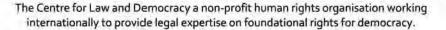
### 1. Introduction<sup>1</sup>

This Submission is pursuant to the ongoing consultation on the Government of Canada's proposed framework for regulating harmful online content. The Government released two documents as part of this consultation: a discussion paper, which outlines the Government's broad proposals,<sup>2</sup> and a technical paper,<sup>3</sup> which contains detailed legislative drafting instructions. This Submission collectively refers to both documents as "the proposal" but focuses on the technical paper to assess the proposal's specific features.

Addressing harmful content online is one of the most controversial topics in the world. While the widespread distribution and amplification of online content by social media companies have created unprecedented opportunities for people to connect and express themselves, the dark side of that freedom has become increasingly evident. Social media companies have been implicated in events such as the genocide of the Rohingya in Myanmar<sup>4</sup> and the 6 January 2021 Capitol riot in Washington D.C.<sup>5</sup> Accordingly, many countries, such as Singapore,<sup>6</sup> Nicaragua<sup>7</sup> and Ethiopia,<sup>8</sup> have introduced a wide array of laws and measures to regulate online content and social media companies.

Canada's proposal to regulate harmful content online is a mixed bag in terms of compliance with human rights. For instance, the proposed user-flagged content moderation system contains several positive features, notably the decoupling of social media companies' initial content moderation decisions from liability<sup>9</sup> and the independence of the various regulatory

<sup>&</sup>lt;sup>9</sup> As explained below, the technical paper requires social media companies to make decisions about whether content is harmful content, but does not impose fines if those decisions are incorrect.



<sup>&</sup>lt;sup>1</sup> This work is licensed under the Creative Commons Attribution-Non Commercial-ShareAlike 3.0 Unported Licence. You are free to copy, distribute and display this work and to make derivative works, provided you give credit to Centre for Law and Democracy, do not use this work for commercial purposes and distribute any works derived from this publication under a licence identical to this one. To view a copy of this licence, visit: http://creativecommons.org/licenses/by-nc-sa/3.0/.

<sup>&</sup>lt;sup>2</sup> Canadian Heritage, Have your say: the Government's proposed approach to address harmful content online: discussion guide, 29 July 2021, https://www.canada.ca/en/canadian-heritage/campaigns/harmful-onlinecontent/discussion-guide.html.

<sup>&</sup>lt;sup>3</sup> Canadian Heritage, Have your say: Government's proposed approach to address harmful content online: technical paper, 29 July 2021, https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html.

<sup>\*</sup> UN Human Rights Council, Report of the independent international fact-finding mission on Myanmar, 18 September 2018, para. 74, https://ap.ohchr.org/documents/dpage\_e.aspx?si=A/HRC/39/64.

<sup>&</sup>lt;sup>5</sup> See, for example, Rory Cellan-Jones, "Tech Tent: Did social media inspire Congress riot?", BBC News, 8 January 2021, https://www.bbc.com/news/technology-55592752.

<sup>&</sup>lt;sup>6</sup> Protection from Online Falsehoods and Manipulation Act 2019, No. 18 of 2019, section 7, https://sso.agc.gov.sg/Acts-Supp/18-2019

<sup>&</sup>lt;sup>7</sup> Ley N. 1042 (Ley Especial de Ciberdelitos), 27 October 2020, Article 30,

http://legislacion.asamblea.gob.ni/normaweb.nsf/(\$All)/803E7C7FBCF44D7706258611007C6D87

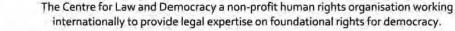
<sup>&</sup>lt;sup>8</sup> Hate Speech and Disinformation Prevention and Suppression Proclamation No. 1185/2020, Articles 5, 7, https://www.article19.org/wp-content/uploads/2021/01/Hate-Speech-and-Disinformation-Prevention-and-Suppression-Proclamation.pdf,

bodies that would be set up by the Act.<sup>10</sup> However, the proposal also contains several highly problematic features that should be overhauled, such as a vague scope of applicability that appears to include some private communications;<sup>11</sup> an unjustifiable 24-hour deadline for social media companies to take measures against harmful content;<sup>12</sup> an ill-defined obligation for social media companies to monitor and takedown harmful content proactively;<sup>13</sup> and an obligation for social media companies to proactively report content to law enforcement bodies, which requires them to make determinations about whether content that is hosted on their platforms is evidence of the commission of a crime.<sup>14</sup> Other aspects of the proposal are not inherently unacceptable but should be tweaked further, such as the definitions of hate speech<sup>15</sup> and terrorist content<sup>16</sup> and the approach to website blocking.<sup>17</sup>

This Submission assesses the proposal from the perspective of international human rights standards, although the Canadian constitutional framework and some laws and jurisprudence are briefly referenced. The Submission starts by laying out the key applicable international legal framework and the relevant human rights engaged by the proposal. Next, the Submission assesses the proposed definitions of harmful content, suggesting tweaks to the definitions for terrorist content and hate speech. The Submission then examines the scope of the proposal, arguing that it should be adjusted to exclude all private communications from its ambit. At this point, the Submission briefly reviews the four new regulatory bodies relevant to the proposal, finding that their independence from government through the Governor-in-Council (GIC) appointments process is key to the successful functioning of the proposal.

The Submission then discusses three additional substantive issues, starting with the userflagged content moderation system, finding that it is largely in line with international standards, with the glaring exception of the 24-hour requirement to address content, which will result in a high rate of erroneous decisions at first instance and worsen an already excessive caseload for the Digital Recourse Council of Canada (Digital Recourse Council or Council), the new content moderation body. The Submission then examines the proposed obligations for online communication service providers (OCSPs) to proactively monitor content for removal and reporting to law enforcement, arguing that these obligations should be removed as they undermine privacy and over-incentivise content removal and reporting. The Submission concludes by recommending that further safeguards be built into the proposed system of website blocking.

<sup>17</sup> Technical paper, ss. 120-123.



<sup>&</sup>lt;sup>10</sup> Technical paper, ss. 36-38 and 46-48.

<sup>11</sup> Technical paper, ss. 2-3.

<sup>12</sup> Technical paper, s. 11.

<sup>&</sup>lt;sup>13</sup> Technical paper, s. 10.

<sup>14</sup> Technical paper, ss. 20, 22.

<sup>&</sup>lt;sup>15</sup> Technical paper, s. 8.

<sup>&</sup>lt;sup>16</sup> Technical paper, s. 8.

## 2. Applicable Legal Framework and Relevant Human Rights

### 2.1. Freedom of Expression

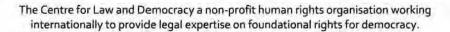
Article 19 of the International Covenant on Civil and Political Rights (ICCPR),<sup>18</sup> ratified by Canada in 1976, is the primary source of international human rights law's protection for freedom of expression. Article 19(2) of the ICCPR provides: "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds..." It is plain that this right will be substantially engaged in any attempt to regulate online content; not just for the impact on would-be expressers of online content but also on the many users who have a right to receive that information.

The right to freedom of expression is not absolute under international human rights law. Restrictions of that right must pass the three-part test outlined in Article 19(3) of the ICCPR. Any restriction must by "provided by law", which means that it must be authorised by a validly passed law and be formulated with sufficient precision to enable individuals who are subject to it to regulate their conduct accordingly.<sup>19</sup> Second, the restriction must seek to protect at least one of the legitimate interests listed in Article 19(3): public order, public health, public morals, national security or the rights and reputations of others. Third, the restriction must be necessary to protect that interest which, among other things, includes an element of proportionality.<sup>20</sup>

The content of the protection in Article 19 of the ICCPR has been further developed and fleshed out in standards issued by a variety of international authorities, such as General Comment 34 of the UN Human Rights Committee, the treaty monitoring body for the ICCPR, and the Joint Declarations and thematic reports of the special international mandates on freedom of expression from the UN, Organization for Security and Co-operation in Europe (OSCE), African Union and the Organisation of American States (OAS).<sup>21</sup> This analysis draws on all of these documents.

While this Submission focuses on international human rights law, it is worth noting that freedom of expression is domestically protected in section 2(b) of Canada's constitutional Canadian Charter of Rights and Freedoms (Charter).<sup>22</sup> As a preliminary note, the above-stated international law test for protecting freedom of expression forms a floor for the

<sup>&</sup>lt;sup>22</sup> Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.



<sup>&</sup>lt;sup>18</sup> UN General Assembly Resolution 2200A (XXI), 16 December 1966, in force 23 March 1976.

<sup>&</sup>lt;sup>19</sup> UN Human Rights Committee, General Comment No. 34, Article 19: Freedoms of opinion and expression, 12 September 2011, para. 25, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

<sup>&</sup>lt;sup>20</sup> Ibid., para 34.

<sup>&</sup>lt;sup>21</sup> For a full list of the Joint Declarations, see: https://www.osce.org/fom/66176.

Charter's domestic protection, as stated by Dickson C.J. in *Re: Public Service Employee Relations Act (Alta.)*:

The content of Canada's international human rights obligations is, in my view, an important indicia of the meaning of "the full benefit of the *Charter*'s protection." I believe that the *Charter* should generally be presumed to provide protection at least as great as that afforded by similar provisions in international human rights documents which Canada has ratified.<sup>23</sup>

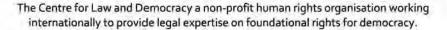
The section 2(b) Charter analysis involves two steps. The first step is ascertaining whether there is a *prima facie* breach of freedom of expression.<sup>24</sup> The question then shifts to whether the *prima facie* breach can be justified under s. 1 of the Charter, which provides that the rights guaranteed by it may be subject to "reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society." This implications of this were elaborated in some detail in the well-known case of *R. v. Oakes.*<sup>25</sup>

#### 2.Z. Privacy

The right to privacy is protected in Article 17 of the ICCPR, which provides: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." Interferences with this right are only permitted where "authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant", is in pursuit of "a legitimate aim" and "meet[s] the tests of necessity and proportionality."<sup>26</sup> Privacy and freedom of expression are interlinked, <sup>27</sup> since privacy "may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities" and "be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality."<sup>28</sup>

As with freedom of expression, the contents of the right to privacy have been further fleshed out in a variety of international statements, including the UN Human Rights Committee's General Comment 16,<sup>29</sup> and the thematic reports of the UN special mandates

https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/1\_Global/INT\_CCPR\_GEC\_6624\_E.doc



<sup>23 [1987] 1</sup> SCR 313, para. 59.

<sup>&</sup>lt;sup>24</sup> See, for example, Canadian Broadcasting Corp. v. Canada (Attorney General), 2011 SCC 2; and Montréal (City) v. 2952-1366 Québec Inc., [2005] 3 S.C.R. 141.

<sup>25 [1986] 1</sup> S.C.R. 103.

<sup>&</sup>lt;sup>26</sup> Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 23 September 2014, para. 30, https://digitallibrary.un.org/record/781159/files/A\_69\_397-EN.pdf.

<sup>&</sup>lt;sup>27</sup> See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, para. 79, https://undocs.org/A/HRC/23/40.

<sup>&</sup>lt;sup>28</sup> Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 22 May 2015, para. 12, https://undocs.org/A/HRC/29/32.

<sup>&</sup>lt;sup>29</sup> 8 April 1988,

on the right to privacy and other privacy-relevant mandates such as the promotion and protection of human rights and fundamental freedoms while countering terrorism.

Domestically, privacy is protected in s. 8 of the *Charter*, which provides: "Everyone shall have the right to be secure against unreasonable search and seizure." This right has been interpreted by the Supreme Court of Canada to include a right to privacy (an unreasonable search being a breach of privacy) that extends online. Indeed, the Supreme Court of Canada has recognised that aspects of informational privacy are especially important in the context of the Internet.<sup>30</sup> The s. 8 analysis comprises of two steps. First, there should be an assessment whether there has been a search or a seizure, requiring an assessment of whether there is a reasonable expectation of privacy in relation to the subject matter of the search or seizure.<sup>31</sup> If so, the second step assesses whether that search or seizure was reasonable, which comprises an analysis of whether the search or seizure was prescribed by law, whether the law was reasonable and whether the manner of the search or seizure was reasonable.<sup>32</sup>

#### 2.3. The Rights of Others

It is important to acknowledge that freedom of expression and privacy are not the only rights at play in this proposal. Social media regulation can affect the free expression and privacy of expressers of content, but various other rights – notably those of the victims of harmful content – are also relevant. Terrorist content, hate speech, incitement to violence and the spreading of child pornography or non-consensual intimate images can have severe impacts on many important human rights.

For instance, hate speech can implicate the rights of others to be free from discrimination, protected in Article 26 of the ICCPR and the subject of an entire UN human rights treaty, the International Convention on the Ending of All Forms of Racial Discrimination (ICERD).<sup>33</sup> International human rights law considers the prevention of hate speech to be so important that Article 20 of the ICCPR requires States to prohibit hate speech, one of the ICCPR's few positive obligations to restrict speech. Similarly, terrorist content and incitement to violence can implicate others' rights to life and to security of the person, as protected in Articles 6 and 9 of the ICCPR. Content that sexually exploits children and the non-consensual sharing of intimate images can implicate others' rights to be free from cruel, inhuman and degrading treatment under Article 7 of the ICCPR and affect dignity, which is

The Centre for Law and Democracy a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy.

<sup>30</sup> R. v. Spencer, 2014 SCC 43, para. 41, https://scc-csc.lexum.com/scc-csc/scc-csc/en/ltem/14233/index.do.

<sup>&</sup>lt;sup>31</sup> See, for example, R. v. Spencer, ibid., generally.

<sup>32</sup> Ibid.

<sup>33 21</sup> December 1965, United Nations, Treaty Series, vol. 660, p. 195.

not a standalone right under the ICCPR but is at the very core of the concept of human rights<sup>34</sup> and features in the preamble of most international human rights treaties.<sup>35</sup>

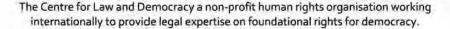
Protecting the rights of others is a legitimate interest which may justify a restriction on freedom of expression and privacy under Articles 19(3) and 17 of the ICCPR respectively.<sup>36</sup> The key question that this Submission addresses is whether all of the proposal's restrictions on free expression and privacy are necessary and proportionate to the protection of legitimate interests, such as the rights of others or public safety.

### 3. The Definitions of Harmful Content

The proposal seeks to target five categories of online "harmful content", each of which largely tracks five categories of content that are already illegal under Canadian law: child sexual exploitation, terrorist content, incitement to violence, hate speech and the non-consensual sharing of intimate images.<sup>37</sup> The Act's definitions "borrow from the Criminal Code<sup>38</sup> but are "adapted to the regulatory context".<sup>39</sup> The only specific example that the technical paper provides of how this adaptation might look pertains to child sexual exploitation. The Act would cover material related to child sexual exploitation that may not constitute a criminal offence but still be harmful to children and victims when posted on an online communication service (OCS), such as screen shots of child porn videos that do not include the criminal activity but "refer to it obliquely".<sup>40</sup>

The five categories of harmful content must be sufficiently narrowly defined to pass the ICCPR's Article 19(3) test that limitations be "provided by law" and the Charter's s. 1 test that limits be "prescribed by law", both of which prohibit restrictions which are unduly vague. Most of the definitions are indeed sufficiently precise, with the exception of "terrorist content". The definition of "hate speech" is sufficiently precise, but given its notoriously subjective nature, its definition should specifically mention international standards on hate speech, such as the Rabat Plan of Action,<sup>41</sup> to guide OCSPs' content moderators and the Digital Recourse Council.

https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat\_draft\_outcome.pdf.



<sup>&</sup>lt;sup>34</sup> UN Office of the High Commissioner for Human Rights, Universal Declaration of Human Rights – in six crosscutting themes, 1996 – 2021, https://www.ohchr.org/en/udhr/pages/crosscuttingthemes.aspx.

<sup>&</sup>lt;sup>35</sup> Including the ICCPR and Universal Declaration of Human Rights (UDHR).

<sup>&</sup>lt;sup>36</sup> See note 27, para. 28.

<sup>&</sup>lt;sup>37</sup> Technical paper, s. 8.

<sup>38</sup> R.S.C., 1985, c. C-46.

<sup>39</sup> Technical paper, s. 8.

<sup>40</sup> Technical paper, s. 8.

<sup>&</sup>lt;sup>41</sup> UN General Assembly, Annual report of the United Nations High Commissioner for Human Rights: Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, pp. 6 – 15, 11 January 2013,

#### 3.1. Terrorist Content

The technical paper does not provide a precise definition for "terrorist content", only explaining that such content is the kind which "actively encourages terrorism and which is likely to result in terrorism."<sup>42</sup> This definition is too flexible, leaving room to argue, for instance, that certain political or religious opinions may not advocate for violence but encourage terrorism because they are uttered in fervent support of ideologies that have been associated with or co-opted by terrorists. Accordingly, the special international mandates on freedom of expression have explained that "Criminal responsibility for expression relating to terrorism should be limited to those who incite others to terrorism; vague concepts such as glorifying', 'justifying' or 'encouraging' terrorism should not be used."<sup>43</sup> While the proposal's prohibition of terrorist content pertains to regulatory rather than criminal responsibility, a more precise definition is still needed for the definition to pass the "provided by law" requirement of the ICCPR.

The technical paper does state that all the definitions of harmful content will be based on corresponding Criminal Code offences. However, it does not state precisely which terrorism-related offence in the Criminal Code the "terrorist content" restriction will be based on. Part II.i of the Criminal Code contains numerous terrorist-related offences, such as counselling<sup>44</sup> or facilitating terrorism,<sup>45</sup> although "terrorist content" is not defined. Terrorist content should be restricted to content which incites terrorist activities, with "terrorist activities" following the definition in s. 83.01(1)(b) of the Criminal Code. That definition requires an intention to cause serious bodily harm or death to a person by violence or to cause a serious risk of harm to the health and safety of the public, bringing it largely in line with the model definition of terrorism adopted by the UN High Level Panel on Threats, Challenges and Change.<sup>46</sup> To make sure that legitimate political, religious or ideological speech is not caught by the definition, the definition of "terrorist content" should also contain the following safeguard, adapted from s. 83.01(1.1) of the Criminal Code on terrorist activities:

For greater certainty, the mere expression of a political, religious or ideological thought, belief or opinion does not constitute terrorist content.

3.2. Hate Speech

The Centre for Law and Democracy a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy.

<sup>42</sup> Technical paper, s. 8.

<sup>&</sup>lt;sup>43</sup> Special international mandates on freedom of expression at the UN, OSCE, OAS and ACHPR, Joint Declaration on freedom of expression and responses to conflict situations, 4 May 2015, s. 3(b), http://www.law-democracy.org/live/wp-content/uploads/2015/05/JD-2015.final\_Eng\_.pdf.

<sup>44</sup> Criminal Code, s. 83.221.

<sup>45</sup> Criminal Code, s. 83.19.

<sup>&</sup>lt;sup>46</sup> Report of the High-level Panel on Threats, Challenges and Change: A more secure world: our shared responsibility, 2 December 2004, para. 164(d), <u>https://undocs.org/A/59/565</u>.

The technical paper defines hate speech in accordance with the definition in Bill C-36, which proposes amendments to the Canadian Human Rights Act.<sup>47</sup> The technical paper also states that the definition of hate speech must be in line with the jurisprudence of the Supreme Court of Canada, which has held that only the most extreme forms of speech would qualify for this title.<sup>48</sup> However, it would also be useful for the proposal, when made into law, to refer to some of the leading international standards on this issue. For instance, the Rabat Plan of Action,<sup>49</sup> the product of a series of UN-led expert consultations on hate speech, provides a useful six-part test for ascertaining when speech rises to the level of hate speech, focusing on the context, speaker, intent, content and form, likelihood of harm and imminence. The law should refer directly to the Rabat Plan of Action and other international instruments on freedom of expression and hate speech.

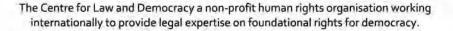
### 4. Who and What Will be Regulated

The main targets of the regulation would be what the proposal calls OCSs and the providers of those services (OCSPs). The proposal would define an OCS as "a service that is accessible to persons in Canada, the primary purpose of which is to enable users of the service to communicate with other users of the service, over the internet"<sup>50</sup> and should exclude services that only enable private communication.<sup>51</sup> This definition would catch all social media services with a public-facing element, such as Facebook, Youtube or Twitter. However, it is unclear whether this proposed definition would cover all of the services of dual-function OCSPs which provide both public-facing and private communications, such as the direct messaging systems of Instagram and Facebook Messenger. This is a reasonable interpretation since the proposed definition would only exclude services that exclusively enable private communications.

It is also unclear how the GIC, in consultation with the Digital Safety Commissioner of Canada (Digital Safety Commissioner, one of the newly created regulatory bodies), will define a "private communication" through regulation.<sup>52</sup> For instance, while services such as Whatsapp and Signal are generally understood to be for wholly private communications, they do allow for one-to-many communications through chat groups or message forwarding. The definition of "private communication" should thus be carefully tailored to

https://parl.ca/Content/Bills/432/Government/C-36/C-36\_1/C-36\_1.PDF.

<sup>&</sup>lt;sup>52</sup> Technical paper, s. 3(c).



<sup>&</sup>lt;sup>47</sup> R.S.C., 1985, c. H-6, https://laws-lois.justice.gc.ca/PDF/H-6.pdf; An Act to amend the Criminal Code and the Canadian Human Rights Act and to make related amendments to another Act (hate propaganda, hate crimes and hate speech), Second Session, 43<sup>rd</sup> Parliament, First Reading, 23 June 2021, s. 13,

<sup>&</sup>lt;sup>48</sup> Saskatchewan (Human Rights Commission) v. Whatcott, 2013 SCC 11, paras. 57 and 116, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/12876/index.do.

<sup>49</sup> See note 41.

<sup>&</sup>lt;sup>50</sup> Technical paper, s. 2.

<sup>&</sup>lt;sup>51</sup> Technical paper, s. 2.

ensure that the Act considers such services to be wholly private and thus exempted from regulation.

In any case, the proposal would empower the GIC, in consultation with the Digital Safety Commissioner, to use regulations to extend the Act's applicability to certain services that do not meet the definition of an OCS if the GIC "is satisfied that there is a significant risk that harmful content is being communicated on the category of services or that specifying the category of services would further the objectives of this Act".<sup>53</sup> This would allow the GIC to expand coverage of the proposed Act to any other service, including private communication services, such as Whatsapp or Signal.

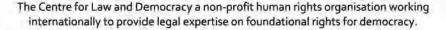
The proposal would oblige OCSPs to create a user-flagging content moderation system for harmful content<sup>54</sup> and to proactively monitor and make the five categories of harmful content inaccessible, including the use of automated systems (these obligations are detailed in greater depth in sections 6 and 7 of this Submission respectively).<sup>55</sup>

Subjecting private messaging services to these obligations would open a Pandora's box of privacy issues. For instance, the obligation on OCSPs to proactively monitor and report content to law enforcement is already problematic for freedom of expression when applied to public content, as explained below. However, if this obligation is applied to private messaging content, it would require OCSPs to monitor the private communications of all their users to identify harmful content and report some of that content to law enforcement. That would essentially be a form of mass surveillance that would be a flagrant violation of the privacy rights of millions of Canadian social media users and a gross breach of Canada's obligations to refrain from arbitrary interferences with privacy under Article 17 of the ICCPR. As stated by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism:

The hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether. By permitting bulk access to all digital communications traffic, this technology eradicates the possibility of any individualized proportionality analysis. It permits intrusion on private communications without independent (or any) prior authorization based on suspicion directed at a particular individual or organization.<sup>56</sup>

Including private messaging content would also create serious feasibility issues. Currently, the major social networks are already struggling with the immense burden of monitoring

<sup>&</sup>lt;sup>56</sup> Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 23 September 2014, para. 12, http://s3.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf.



<sup>53</sup> Technical paper, s. 3.

<sup>54</sup> Technical paper, s. 11.

<sup>55</sup> Technical paper, s. 10.

and moderating public content.<sup>57</sup> Including all of the private messaging on their platforms would quite clearly be beyond the capacity of OCSPs and would likely massively overload the user-flagging system and the caseload of the Digital Recourse Council. The Act should contain language that clearly excludes all forms of private messaging from its ambit in all circumstances.

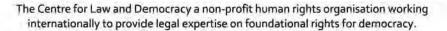
### 5. Five New Regulatory Bodies

The Act creates four new regulatory bodies to fulfil its aims: the Digital Safety Commissioner, the Digital Safety Commission, the Digital Recourse Council and the Advisory Board. A fifth relevant body, the Personal Information and Data Protection Tribunal, would be responsible for oversight of the penalties recommended by the Digital Safety Commissioner but is proposed in another bill, Bill C-11, which is currently before the House of Commons.<sup>58</sup>

The independence of the three bodies that have enforcement or adjudicatory functions – the Digital Safety Commissioner, Digital Recourse Council and the Personal Information and Data Protection Tribunal – is key to the appropriate functioning of the Act. For instance, the process for resolving appeals from content moderation systems will only meet international standards if the body deciding the appeals is free from political and commercial influence.<sup>59</sup> It is not so crucially important that the other two entities – the Advisory Board and the Digital Safety Commission – be independent of government, as the former merely serves a high-level advisory role<sup>60</sup> while the latter plays a supporting role for the other three bodies created by the Act,<sup>61</sup> although independence for both is still still highly advisable.

All three of the proposed adjudicatory and enforcement bodies appear to be sufficiently insulated from political or commercial influence. In terms of freedom from political influence, members of all three bodies are selected through Canada's GIC appointments process;<sup>62</sup> while the GIC is a political body, candidates must undergo a rigorous vetting process that ensures that they are ultimately chosen on the basis of merit and that adequate

<sup>62</sup> Technical paper, ss. 36-37 and 46-47. C-11, Part 2, s. 6.



<sup>&</sup>lt;sup>57</sup> See, for example, John Koetsier, "Report: Facebook Makes 300,000 Content Moderation Mistakes Every Day", Forbes, 9 June 2020, https://www.forbes.com/sites/johnkoetsier/2020/06/09/300000-facebook-content-moderation-mistakes-daily-report-says/?sh=619f3dee54d0.

<sup>&</sup>lt;sup>58</sup> An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts, Second Session, 43<sup>rd</sup> Parliament, First Reading, 17 November 2020, https://parl.ca/Content/Bills/432/Government/C-11/C-11\_1/C-11\_1.PDF.

<sup>&</sup>lt;sup>59</sup> Special international mandates on freedom of expression at the UN, OSCE, OAS and ACHPR, Joint Declaration on media independence and diversity in the digital age, 2 May 2018, s. 1(b)(v), https://www.law-democracy.org/live/wp-content/uploads/2018/12/mandates.decl\_.2018.media-ind.pdf.

<sup>&</sup>lt;sup>60</sup> Technical paper, s. 75.

<sup>61</sup> Technical paper, s. 60.

consideration is also given to diversity.<sup>63</sup> A specific subcategory of GIC appointees exists to further ensure independence from government, the GCQ category, for whom salary components cannot be determined by the GIC (unlike other federal government positions, which have a variable performance-based component that is determined by the GIC).<sup>64</sup> The members of the three adjudicatory and enforcement bodies should be GCQ positions, much like the members of Canada's other independent oversight bodies, such as the Canadian Human Rights Commission or the National Parole Board.<sup>65</sup>

In terms of freedom from commercial influence, members of the Digital Safety Commissioner and the Digital Recourse Council cannot be shareholders in an OCS or OCSP and members of all three adjudicatory or enforcement bodies must declare any conflicts of interest they have with regard to matters under their purview.<sup>66</sup>

### 6. The User-flagged Content Moderation System

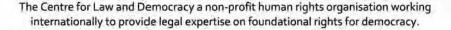
#### 6.1. The Proposed User-flagged Content Moderation System

The proposal would create a new, two-tier system of content flagging and moderation. The first tier is handled by OCSPs, which must create systems that enable their users to flag easily content which they believe falls within the scope of one of the five categories of harmful content.<sup>67</sup> Users who believe that these systems are inadequate may complain to the Digital Safety Commissioner, who may investigate and adjudicate that complaint.<sup>68</sup>

Once a user has flagged content, the OCSP must arrive at a decision within 24 hours on whether the content is harmful, although the GIC can prescribe a different timeline for some categories of content.<sup>69</sup> If the OCSP decides that the content is harmful, it must render it inaccessible to Canadian users; if it decides otherwise; the content may stay up.<sup>70</sup> In all cases, the OCSP must provide notice of its decision to the flagger and the author of the

<sup>63</sup> Government of Canada, Governor-in-Council appointments, 1 Feb 2021, https://www.canada.ca/en/privycouncil/programs/appointments/governor-council-appointments/general-information/appointments.html.
<sup>64</sup> Government of Canada, Terms and conditions applying to Governor in Council appointees, 1 April 2018, https://www.canada.ca/en/privy-council/programs/appointments/governor-council-appointments/compensationterms-conditions-employment/terms-conditions.html.

<sup>&</sup>lt;sup>70</sup> Technical paper, s. 11(b).



<sup>65</sup> Ibid.

<sup>66</sup> Technical paper, ss. 38 and 48; C-11, Part 2, s. 12.

<sup>67</sup> Technical paper, s. 12(a).

<sup>68</sup> Technical paper, ss. 12, 40-44.

<sup>69</sup> Technical paper, s. 11(a).

content.<sup>71</sup> The OCSP must also provide both parties with an option for an internal appeal to the OCSP (the Act's name for this process is "reconsideration").<sup>72</sup>

The second tier of the content moderation system is handled by the Digital Recourse Council. Either party to a content moderation dispute may file a complaint to the Digital Recourse Council if they are dissatisfied with the results of the internal appeal.<sup>73</sup> The Digital Recourse Council has the power to dismiss complaints that are "trivial, frivolous, vexatious, made in bad faith or on other grounds".<sup>74</sup> Once a complaint is filed, both parties must receive notice of the complaint and have the opportunity to make representations, which may include a hearing if the Digital Recourse Council considers that to be in the public interest.<sup>75</sup> These hearings can be private if the Digital Recourse Council and the Digital Safety Commissioner determine that "a public hearing would not be in the public interest, including where there is a privacy interest, national security interest, international relations interest, national defence interest, or confidential commercial interest."<sup>76</sup>

If the Digital Recourse Council finds that the content does not fall within one of the five categories of harmful content, it communicates its decision to all parties; the OCSP may then leave the content up or still decide to make the content inaccessible in accordance with its internal guidelines.<sup>77</sup> If the Digital Recourse Council finds that the content does fall within one of the five categories of harmful content, it communicates its decision to all parties and orders the OCSP to make the content inaccessible in Canada, if the OCSP has not already done so.<sup>78</sup> This order is to be shared with the Digital Safety Commissioner, who is to monitor the OCSP's compliance with the inaccessibility order.<sup>79</sup>

A failure to comply with a Digital Recourse Council's inaccessibility order is one of the bases for levying administrative fines of up to 3% of an OCSP's gross global revenue or up to ten million Canadian dollars, whichever is higher.<sup>80</sup> Failing to comply with an inaccessibility order could also constitute a criminal offence under the Act which can incur fines of 4-5% of an OCSP's gross global revenue or 20-25 million Canadian dollars,<sup>81</sup> although the proposal does not make it clear what threshold distinguishes the administrative penalty from the criminal penalty. To be clear, these fines are incurred if an OCSP defies an inaccessibility order issued by the Digital Recourse Council; the technical

- <sup>71</sup> Technical paper, s. 12(b).
- 72 Technical paper, s. 12(c).
- 73 Technical paper, s. 49.
- 74 Technical paper, s. 52.
- 75 Technical paper, s. 53.
- 76 Technical paper, s. 59.
- 77 Technical paper, s. 54.
- 78 Technical paper, s. 55.
- 79 Technical paper, s. 56.
- <sup>80</sup> Technical paper, s. 108.
- <sup>81</sup> Technical paper, s. 119.



The Centre for Law and Democracy a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy.



paper does not contemplate penalties where OCSPs issue initial content moderation decisions which are later overturned by the Digital Recourse Council.

#### 6.2. Assessment of the User-Flagged Content Moderation System

The proposed user-flagged system of content moderation contains several useful protections for freedom of expression. Crucially, the system does not link the OCSPs' initial content moderation decision to liability, even if that decision is later reversed on appeal, thereby removing any incentive to be over-inclusive when removing content. Both the author of the flagged content and the flagging user have equal appeal rights,<sup>82</sup> which ensures procedural fairness for users and also likely reduces the likelihood of OCSP bias towards either content removals or takedowns for purposes of avoiding downstream engagement in the process. Notice to all concerned parties must be issued at every major step of the decision-making process,<sup>83</sup> and appeals from content moderation decisions will be handled by an independent regulator, the Digital Recourse Council, with further recourse to judicial review by the Federal Court of Canada.<sup>84</sup>

However, one glaring problem in the user-flagging system is the 24-hour deadline to reach a decision in respect of all five types of harmful content. This ignores key differences between types of content and the relative urgency with which they need to be addressed. Overall, it is almost certain to result in poorer quality decisions across the board than if more time was allocated for this. While the salutary features of the system mentioned in the previous paragraph mean that decisions will not necessarily be poorer in a certain direction – for example, in the direction of over-removal – they will nonetheless be wrong more often.

The technical paper does not offer any justification for why the 24-hour deadline is necessary for any – let alone all five – of the categories of harmful content. It is true that in the case of child sexual exploitation, where the content is relatively easy to identify and normally easy at least to distinguish from political or other forms of public interest speech, and where its ongoing dissemination is especially harmful, a 24-hour deadline may be justifiable. In the case of non-consensual sharing of intimate images, a 24-hour deadline may also be justifiable given the extreme harm that can result from the dissemination of those images. It may be difficult to distinguish rapidly between consensual and nonconsensual sharing of intimate images, since this assessment requires some analysis of context. However, intimate images, even if consensual, will rarely constitute public interest speech and are in any case already prohibited by the content standards of major social

The Centre for Law and Democracy a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy.

<sup>82</sup> Technical paper, s. 49.

<sup>83</sup> Technical paper, ss. 51, 52,

<sup>84</sup> Federal Courts Act, R.S.C., 1985, c. F-7, s. 18(1), https://laws-lois.justice.gc.ca/PDF/F-7.pdf.

media companies.<sup>85</sup> The significant benefits of legally mandating the rapid removal of nonconsensual intimate images may therefore outweigh the costs of doing so.

However, in the cases of hate speech, terrorist content and incitement to violence, the dividing line will often be hard to draw, making a one-day deadline far too short for a content moderator to arrive at a considered decision. As suggested above, hate speech and terrorist content can be difficult to distinguish from political or religious speech. Incitement to violence is sometimes clear-cut but may also involve complex assessments of nuance. One prominent example is the Facebook Oversight Board's decision to uphold Facebook's ban on US President Trump for alleged incitement to violence over the 6 January 2021 Capitol riot. It took five months for the oversight body to arrive at a decision, which was not unanimous, illustrating the highly subjective and complex nature of labelling speech as incitement to violence.<sup>86</sup> Content moderators cannot consistently make high-quality decisions on these matters within 24 hours. Line content moderators may also take more than 24 hours.

The result will likely be a high proportion of content moderation decisions that are decided incorrectly. It is not clear at this point whether these decisions would, in aggregate, tend towards the over-removal of legitimate content or over-maintenance of harmful content. Since the proposed Act does not levy penalties on OCSPs for making content moderation decisions that are later overturned by the Digital Recourse Council, there are no obvious incentives towards over-removal, although there may well be more subtle ones, such as a tendency to respond to the creaky wheel, i.e. the user who complains about content. Authors raising sensitive issues may also be reluctant to defend their content vigorously, which could again result in a bias within the system. In any case, poor decisions will still harm freedom of expression, since at least a percentage will involve the inappropriate removal of content at the first instance which could only be restored on appeal or perhaps never if no appeal is forthcoming. On the flip side, hurried decisions that lead to harmful content erroneously being left up also defeat the Act's primary purpose of removing harmful content online.

Another negative implication of the 24-hour limit is that more social media users are likely to lose trust in social media companies' content moderation processes. This may be the case whether the user is the author of political content that has been mistaken for terrorist content or a person of colour who has identified racist hat speech that has been left up by a

The Centre for Law and Democracy a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy.

<sup>85</sup> Facebook, Facebook Community Standards: Adult Nudity and Sexual Activity, 2021,

https://transparency.fb.com/policies/community-standards/adult-nudity-sexual-activity/; Twitter, Sensitive media policy, November 2019, <a href="https://help.twitter.com/en/rules-and-policies/media-policy">https://help.twitter.com/en/rules-and-policies/media-policy;</a>; and Tiktok, Community guidelines: Adult nudity and sexual activities, December 2020, <a href="https://www.tiktok.com/community-guidelines?lang=en#30">https://help.twitter.com/en/rules-and-policies/media-policy;</a> and Tiktok, Community guidelines: Adult nudity and sexual activities, December 2020, <a href="https://www.tiktok.com/community-guidelines?lang=en#30">https://www.tiktok.com/community-guidelines?lang=en#30</a>.

<sup>&</sup>lt;sup>86</sup> Facebook Oversight Board, Case decision 2021-001-FB-FBR, 5 May 2021, https://www.oversightboard.com/sr/decision/2021/001/pdf-english.

content moderator forced to make a hasty decision. And rushed first-level decisions will almost certainly lead to far more appeals being lodged with the OCSP's internal appeal process, and potentially with the Digital Recourse Council, especially as users observe a reasonably high rate of initial decisions getting overturned. This, in turn, will increase what can reasonably be expected to be a fairly massive caseload placed on these bodies.

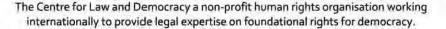
A reasonably obvious solution is to give OCSPs more time to address content that has been flagged as hate speech, incitement to violence or terrorist content, while child sexual exploitation material and non-consensually shared intimate images could still be addressed within 24 hours. A 72-hour initial deadline that can be extended through a simple procedure for a further week if necessary should provide OCSPs with enough time to make considered decisions about content.

#### 6.3. Caseload of the Digital Recourse Council of Canada

The Digital Recourse Council comprises three to five members<sup>87</sup> and is required to review all appeals from OCSPs' initial moderation decisions, with the only limitation being the Council's power to dismiss complaints that are "frivolous, vexatious, trivial, made in bad faith or on other grounds".<sup>88</sup> The GIC may introduce other grounds for dismissing complaints<sup>89</sup> but, otherwise, the Council is required to adjudicate all complaints that have merit. This may be contrasted with the Facebook Oversight Board, which only adjudicates the few cases that are "difficult, significant and globally relevant".<sup>90</sup>

It is not possible to predict with any certainty the volume of complaints that the Council will receive but statistics from other systems given some insight into this. For example, in the 2<sup>nd</sup> quarter of 2021, internally appeals were lodged against about 1,400,000 of Facebook's initial content moderation decisions just regarding hate speech worldwide.<sup>91</sup> Scaling down for Canada's population,<sup>92</sup> that roughly translates into about 77 internal appeals for every day of the year. If just 25% of those internal appeals were subject to complaints before the Council (a potentially conservative estimate, given that this costs nothing), that would be 19 complaints every day just in relation to hate speech, and arising from Facebook alone. Of course scaling of this sort is notoriously unreliable but it seems reasonable to assume that the number of complaints to the Council would be enormous.

<sup>&</sup>lt;sup>92</sup> Worldometer, Canada Population, 21 September 2021, https://www.worldometers.info/world-population/canadapopulation/.



<sup>&</sup>lt;sup>87</sup> Technical paper, s. 46.

<sup>88</sup> Technical paper, s. 52.

<sup>89</sup> Technical paper, s. 52.

<sup>90</sup> Facebook Oversight Board, Appealing Content Decisions on Facebook or Instagram,

https://oversightboard.com/appeals-process/.

<sup>&</sup>lt;sup>91</sup> Facebook, Community Standards Enforcement Report – Hate Speech, August 2021,

https://transparency.fb.com/data/community-standards-enforcement/hate-speech/facebook/.

This has important implications in terms of the operations and budgets of the Council and the Digital Safety Commission that supports it. We note that it is imperative that it be able to process complaints rapidly since, otherwise, wrong decisions – whether to allow harmful content to remain online or to block access to legitimate content – will remain in place, undermining the credibility of the system and harming freedom of expression. In terms of operations, the Council will need to have staff processing complaints, whether or not these are ultimately signed off on by the Council's members, where these staff are housed in the Council itself or in the supporting Digital Safety Commission. To process a large volume of complaints rapidly, that staffing complement would need to be significant. And to process complaints properly, the staff will need to be very professional. All of which suggests that the government should be prepared to commit significant resources to sustain the operations of the Council.

## 7. OCSPs Proactive Obligations

 OCSPs to Take "All Reasonable Measures" to Identify and Make Harmful Content Inaccessible

Alongside the user-flagging content moderation system, the Act also obliges OCSPs to "take all reasonable measures" to identify harmful content on their platforms and to make that content inaccessible in Canada.<sup>93</sup> The technical paper does not provide specifics on what these measures would entail, although it explicitly contemplates the use of automated systems.<sup>94</sup> The Digital Safety Commissioner may prescribe rules in this area by regulation, which presumably covers both what would constitute "all reasonable measures" and how to make content inaccessible.<sup>95</sup> These measures cannot result in discrimination, as described in Canada's anti-discrimination legislation, the Canadian Human Rights Act, but no other constraints are set out here.

There are serious problems with placing legal obligations on OCSPs to monitor content on their systems. The volume of material most OCSPs host means that monitoring can only really be done with automated tools, since there is too much material for humans to monitor, at least for the first pass. Using such tools to identify content that involves child sexual exploitation is relatively less sensitive, since such content is generally easier to identify and more difficult to mistake for public interest content. But using automation to identify hate speech, terrorist content, incitement to violence and the non-consensual sharing of intimate images is highly problematical given that such tools remain relatively

The Centre for Law and Democracy a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy.

<sup>93</sup> Technical paper, s. 10.

<sup>94</sup> Ibid.

<sup>95</sup> Ibid.

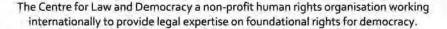
crude.<sup>96</sup> For instance, Facebook, Youtube and Twitter's automated systems have on multiple occasions taken down evidence of mass atrocities and war crimes by misidentifying it as terrorist content or incitement to violence.<sup>97</sup> This is why international standards make it clear that it is not legitimate to place a positive obligation on OCSPs to monitor for illegal content.<sup>98</sup> In this context, the technical paper's specific reference to automated systems is especially troubling, including insofar as it would allow the Digital Safety Commissioner to direct OCSPs specifically to rely on automation for content identification and perhaps even removal.

The allocation of sweeping power to the Digital Safety Commissioner to regulate how OCSPs must proactively identify and remove content is also a violation of Article 19 of the ICCPR, which requires restrictions on freedom of expression to be both provided by law and narrowly tailored. As stated by the UN Human Rights Committee, "A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution."<sup>99</sup> The only constraints that are placed on the exercise of these powers are that they must be "reasonable" and cannot fall foul of non-discrimination protections,<sup>100</sup> which signally fail to meet the standard set out by the Human Rights Committee.

Instead of allocating broad authorisation to the use of automated content identification and removal systems, the proposal should establish guardrails around the use of such systems. Such guardrails might, for example, require initially flagged content to be reviewed by a human being, providing an opportunity to fix automated errors. Automated systems which entail the use of content filtering – the pre-emptive blocking of content triggered by certain metrics, such as keywords – are not legitimate. Such systems, when not controlled by the end-user, have been condemned by the international special mandates as being "a form of prior censorship and not justifiable as a restriction on freedom of expression."<sup>101</sup>

The technical paper is not as clear as it should be regarding the right of users to appeal against measures taken by OCSPs against their content as described above. This seems to be

<sup>&</sup>lt;sup>101</sup> Special international mandates on freedom of expression at the UN, OSCE, OAS and ACHPR, Joint Declaration on Freedom of Expression and the Internet, 1 June 2011, s. 3(b), http://www.law-democracy.org/wp-content/uploads/2010/07/11.06.Joint-Declaration.Internet.pdf.





<sup>&</sup>lt;sup>96</sup> Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018, para. 29, https://documents-dds-

ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement.

<sup>&</sup>lt;sup>97</sup> Human Rights Watch, "Video Unavailable", Social Media Platforms Remove Evidence of War Crimes, 10 September 2020, https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-removeevidence-war-crimes.

<sup>&</sup>lt;sup>98</sup> Special international mandates on freedom of expression at the UN, OSCE, OAS and ACHPR, Joint Declaration on Freedom of Expression and the Internet, 1 June 2011, s. 2(b), <u>http://www.law-democracy.org/wp-content/uploads/2010/07/11.06.Joint-Declaration.Internet.pdf</u>; and Council of Europe, CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, 7 March 2018, s. 1.3.5, https://rm.coe.int/1680790e14.

<sup>99</sup> See note 19, para. 35.

<sup>100</sup> Technical paper, s. 10.

provided for,<sup>102</sup> but any legislation should clarify this in favour of equal rights to appeal for all affected users, whether they are flaggers or authors. It is also important that provision be made for users whose content is affected by OCSP monitoring and proactive content moderation measures to be notified as soon as any decision is made, thereby enabling them to appeal.

#### OCSPs to Have New Reporting Obligations to Law Enforcement and Intelligence Services

OCSPs must also report regularly to the Digital Safety Commissioner on a broad range of data about their services in Canada, including the volume and type of harmful content on them, the volume and type of content they have moderated, the resources and personnel dedicated to content moderation and how they "monetize harmful content".<sup>103</sup> To fulfil these and other obligations, OCSPs must have adequate record management systems and practices in place.<sup>104</sup> These features should be kept within the proposal as they would result in increased transparency about harmful content on OCSPs and measures taken to address it, a positive development.

The second type of reporting obligation is to law enforcement, and the technical paper indicates that the Government of Canada is contemplating two options here.<sup>105</sup> The first option would obligate OCSPs to notify the Royal Canadian Mounted Police (RCMP) if they have reasonable grounds to believe that content that falls within the five categories of harmful content, and is therefore likely criminal in nature, poses an imminent risk of serious harm to any person or property.<sup>106</sup> The second option would obligate OCSPs to report to the relevant law enforcement agency – which could be the RCMP, the Canadian Security and Intelligence Services (CSIS) or others – in respect of certain crimes (to be prescribed by the GIC through regulation) based on content that falls within the five categories of harmful content.<sup>107</sup> Thus, the notification option is only for the RCMP and for content that poses an imminent risk of harm, while the reporting option is for any relevant law enforcement agency and covers prescribed crimes covered by the five categories of harmful content. Both options are to be subject to regulated standards on timing, the type of information to be provided, the thresholds of severity that trigger notifications or reports, and the formats of notifications or reports.<sup>108</sup>

<sup>&</sup>lt;sup>108</sup> Technical paper, s. 20.



The Centre for Law and Democracy a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy.

<sup>&</sup>lt;sup>102</sup> For example in s. 12(c).

<sup>&</sup>lt;sup>103</sup> Technical paper, s. 14.

<sup>&</sup>lt;sup>104</sup> Technical paper, s. 15.

<sup>&</sup>lt;sup>105</sup> Technical paper, s. 20.

<sup>&</sup>lt;sup>106</sup> Technical paper, s. 20(a).

<sup>&</sup>lt;sup>107</sup> Technical paper, s. 20(b).

A key problem here is that OCSPs are required to monitor content in the first place, discussed above, absent which it is not clear how these notification or reporting requirements could be discharged.

A second issue is that these obligations essentially deputise OCSPs to make subjective determinations on law enforcement issues which they are not qualified to do and which are best left up to law enforcement bodies. These include, respectively, whether content poses an imminent risk or harm or represents criminal behaviour. In the exceptional case of the crime of spreading child sexual exploitation content, the benefits of reporting may outweigh the risks, especially given that, as noted earlier, identification is less controversial in this case. Otherwise, however, this sort of reporting obligation is not appropriate. We note that notification or reporting by OCSPs is not value neutral; rather, it will likely trigger a police investigation. As such, unreliable reporting, especially where it is over-inclusive, exposes users to unjustified interactions with law enforcement bodies, which is not legitimate.

The technical paper fails to make it clear what type of information would need to be included in notifications or reports, which is left up to future regulations.<sup>109</sup> We note that this should be limited to the content of the social media post and not include user information, such as name, email address, phone number or IP address. To require the provision of that sort of information to law enforcement officials without judicial authorisation would be a serious breach of the right to privacy under international human rights law. As the UN Human Rights Committee has stated: "[S]ubscriber information may be issued with a warrant only."<sup>110</sup> The technical paper does specifically provide that OCSPs should preserve and retain basic subscriber information that is pertinent to their reporting obligations,<sup>111</sup> which may suggest that this information would only be releasable pursuant to a warrant, but this should be made crystal clear in the wording of the Act.

## 8. Website Blocking

If an OCSP persistently defies orders to block content relating to child sexual exploitation or terrorist content, and if all other enforcement mechanisms have been exhausted, the Digital Safety Commissioner may apply to the Federal Court of Canada to request that

<sup>111</sup> Technical paper, s. 23.

The Centre for Law and Democracy a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy.

<sup>&</sup>lt;sup>109</sup> Technical paper, s. 20.

<sup>&</sup>lt;sup>110</sup> UN Human Rights Committee, Concluding Observations on the Fourth Periodic Report of the Republic of Korea, 3 December 2015, para. 43,

http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhshdNp32UdW56DA%2F SBtN4MHy9iuSMtUiNSvrbV9%2BJuD7JMLvy0Ju%2FXKLNHlCvzsdHK1rJtIsosm9tfQBiOl2kvBgjNYQMFXBklPP6C l8vcuw0.

telecommunications service providers wholly or partially block access to the offending OCSP in Canada.<sup>112</sup>

Website blocking is an extreme measure that can only be justified in highly exceptional circumstances, as the special international mandates on freedom of expression have stated:

Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse.<sup>113</sup>

That said, the proposed modalities for website blocking do contain safeguards. Blocking can only be exceptionally employed against sites that consistently defy orders issued by the Digital Recourse Council with respect to terrorist content or child sexual exploitation,<sup>114</sup> the latter highlighted above by the special mandates as one instance where website blocking could be justified. All other enforcement mechanisms must have been exhausted and the blocking orders can only be issued by the Federal Court of Canada upon an application by the Digital Safety Commissioner.<sup>115</sup> Furthermore, the technical paper states that the Act should direct the Digital Safety Commissioner to ensure that the blocking orders it requests are proportionate, taking into account the risk of excessive blocking.<sup>116</sup>

Further tweaks are nonetheless needed to strengthen safeguards for freedom of expression. While the language about blocking orders needing to be proportionate is welcome, more specific safeguards are needed given the extreme nature of website blocking. Either the Act or its regulations should address the technical challenges of blocking individual pages of a website, rather than a whole OCSP.<sup>117</sup> Where it is technically impossible to tailor blocking orders, considerations of proportionality may require orders to err on the side of leaving websites up instead of blocking them. The law should also clearly require the Digital Safety Commissioner to maintain a public and up-to-date list of blocked sites.

Finally, for the website blocking regime to be legitimate, it is crucial that the problems with the vague definition of terrorist content, highlighted in s. 3.1 of this Submission, are addressed. If the Act fails to provide a clear definition of terrorist content or if that definition is not strictly restricted to content which incites terrorist activities, then it would enable the blocking of websites that host content which is controversial but not prohibitable under international law.

The Centre for Law and Democracy a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy.



<sup>&</sup>lt;sup>112</sup> Technical paper, s. 120.

<sup>&</sup>lt;sup>113</sup> See note 101, s. 3(a).

<sup>114</sup> Technical paper, s. 120.

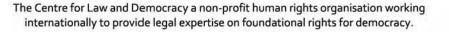
<sup>115</sup> Ibid.

<sup>&</sup>lt;sup>116</sup> Technical paper, s. 121.

<sup>&</sup>lt;sup>117</sup> Internet Society, Internet Society Perspectives on Internet Content Blocking: An Overview, 24 March 2017, https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/.

## Recommendations

- The definition of "terrorist content" should be strictly limited to "content that incites terrorist activities" and the definition of terrorist activities should be linked to or mirror the definition in s. 83.01(1)(b) of the Criminal Code, including the safeguard in s. 83.01(1.1) of the Code.
- The definition of "hate speech" should incorporate by reference international human rights standards on hate speech and freedom of expression.
- The scope of the legislation should clearly exclude all private communications in all circumstances.
- Members of the Digital Safety Commissioner, Digital Recourse Council and the Personal Information and Data Protection Tribunal should be appointed as GCQ-level positions to promote their independence from government.
- The 24-hour requirement to address harmful content should only apply to content about child sexual exploitation and the non-consensual sharing of intimate images. For hate speech, incitement to violence and terrorist content, the deadline should be 72hours and OCSPs should be able to extend that by an additional week in challenging cases.
- Significant resources should be allocated to the Digital Recourse Council so that it can handle its caseload in a timely manner.
- The legal obligations for OCSPs to proactively monitor and remove content should be removed, perhaps other than for child sexual exploitation content.
- The legal obligations for OCSPs to proactively report or notify law enforcement bodies about the content found on their platforms should be removed.
- The rules on blocking of websites should contain additional safeguards for freedom of expression and transparency, such as directing the Digital Safety Commissioner to maintain a public list of blocked sites and rules that require careful tailoring, within technical constraints, of any blocking measures to ensure that blocking is proportionate and, in particular, that innocent content is not blocked.





September 13, 2021

# The Federal Government's Proposal to Address Online Harms: Explanation and Critique

By: Darryl Carmichael and Emily Laidlaw

Commented On: The Federal Government's proposed approach to address harmful content online

In late July, the Federal Government introduced its <u>proposal</u> for online harms legislation for feedback. It comprises a <u>discussion paper</u> outlining the government's approach to regulating social media platforms and a <u>technical paper</u> that provides more detail on the substance of the proposed law. The proposal is part of a suite of law reform efforts by the Canadian government concerning what can broadly be categorized as platform regulation and content regulation issues. They include Bill C-10 to reform broadcasting laws, which stalled when it hit the Senate floor (for now at least) and <u>proposed legislation</u> to combat hate speech and hate crimes. The timing of the online harms and hate speech proposals has been a point of contention so close to the election call. Regardless of the election result in September, it is worthwhile analyzing this proposal because the Canadian government will need to prioritize law reform in this area. Online harms legislation is sweeping the globe, and Canada is well overdue to address these issues. For better or worse (as remains to be seen), new laws have been proposed or passed in <u>Europe</u>, the <u>United Kingdom</u> (UK), <u>Australia</u>, India, and <u>Turkey</u>, to name a few.

All blog posts include a caveat that the analysis is not fulsome, but it seems crucial to emphasize that here. The scope of online harms is broad and can include anything and everything posted online, and the regulatory environment is global, even if what is discussed is domestic law. Indeed, the broad scope of this proposal is a point of criticism, with scholars such as <u>Cynthia Khoo</u> arguing that this should be broken down into subject-matter specific legislation. All this to say that what is offered here are the highlights of some of the key issues of debate and concern.

The Department of Heritage is open for feedback on the proposal until September 25<sup>th</sup>, depending on the election result. Therefore, this post is organized to provide such feedback. The analysis focuses on some of the major points of reform: scope and definitions, the proposed regulator, proactive monitoring, 24-hour takedown requirements, website blocking, mandatory reporting, and transparency obligations. Each point is explained and critiqued, and recommendations are made to address the criticisms. Because of the nature of this post and the breadth of the proposal, many of the recommendations are relatively general and have the same theme: implementation of this proposal needs to be slowed down and significant consultation undertaken.

By way of introduction, the proposal aims to regulate social media platforms concerning how they moderate certain types of harmful content: terrorist content, content that incites violence, hate speech, non-consensual sharing of intimate images, and child sexual exploitation content. It proposes the creation of a new regulator, the Digital Safety Commission, which would provide

THE UNIVERSITY OF CALGARY FACULTY OF LAW BLOG

recourse concerning specific items of content, oversee and investigate platforms concerning their moderation systems, and enable major administrative penalties to be levied against non-complying platforms. The proposal would also impose significant new obligations on platforms, such as to action content within 24 hours of it being flagged and to proactively monitor content on their services.

To set the scene of the complexity of content moderation, let's use a <u>famous example</u> in content moderation circles. In 2016, Facebook famously grappled with whether to remove a Pulitzer Prizewinning photograph of the "Napalm Girl". We all know the photo. It is the haunting image of a naked and sobbing Vietnamese girl running from a napalm attack. It was shared on Facebook as an example of photographs that had changed the history of warfare. Facebook initially removed the photo, and after severe criticism, reversed its decision and reinstated it. However, the decision of what to do is not as easy as it might seem. It is an iconic and newsworthy photo of historical significance, but it is also a brutal and intimate image of a child at one of the most horrific moments in their lives. Years later, the girl depicted in the photo, now 44 years old, <u>commented</u>, "[t]he more the picture got famous, the deeper the cost to my private life." But someone had to make that decision – and for platforms, it is a content moderator, automated system, or both depending on how their system is designed.

Let's play out how this image might be treated in this proposal. One of the categories of harm in the proposal is intimate images as defined in the *Criminal Code*, <u>RSC 1985, c C-46</u>, "but adapted to a regulatory context" (technical paper, para 8), which presumably means a broader rather than a narrower scope. The photo might be an intimate image pursuant to s 162.1 of the *Criminal Code* because it shows nudity and was taken and shared without consent. It does not depict a sexual activity. However, depiction of sexual activity is not required in the definition an of intimate image. Rather, s 162.1(2) requires the depiction of nudity *or* sexual activity, although the section is bundled under the heading of "Sexual Offences" with crimes such as sexual exploitation and voyeurism. The photo must also be shared in circumstances giving rise to a reasonable expectation of privacy, and that is a matter of debate in these circumstances. There is a defence that the conduct serves the public good. One argument is that taking and sharing this image – by the original photographer and by the user on Facebook – serves the public good. However, a public good defence is not a newsworthy defence, although they overlap. The question is whether there is some public benefit. Certainly, there is a strong argument here that taking and sharing the image is a public good, but it is not obvious given that this is a child and the intimate circumstances.

Now let's take a step back. This is not a decision by the police about whether to investigate or the Crown about whether to prosecute an individual nor is this a decision by a court whether to convict, all of which would be highly unlikely. This is a social media platform deciding whether to remove content from circulation in light of its obligations under this new online harms proposal if made law. Platforms would have 24 hours from the moment the content is flagged to make the assessment. This should be understood in the context that hundreds of million photos are posted to Facebook daily. Conservative advice to the platform would be to take the image down. But that requires the image to be de-contextualized and advice provided purely based on risk avoidance, and that is the problem. The risk to the platform is a potentially enormous administrative penalty, even if remote, and while the image is defensible, it is not obviously so. Blunt legislation forces

THE UNIVERSITY OF CALGARY FACULTY OF LAW BLOG

blunt responses by those regulated by it, and we all lose because the richness and complexity of how we converse will be neutered.

## Scope & Definitions

The proposal sets its sights on Online Communication Services (OCS) and providers of these services (OCSPs). The proposal restricts its application to services whose primary purpose is to enable communication with other users of the service over the internet. This will explicitly exclude private communications, telecommunication service providers, search engines, caching services and potentially others to be specified later (technical paper, paras 1-6). The result is that the proposal targets social media like TikTok, Facebook, and Twitter but would not include WhatsApp, review sites, or comment sections on news pages. Given the onerous obligations and sizeable administrative penalties, this perhaps makes sense. However, this approach might not help achieve the objective of reducing harmful content online.

It is unclear if only major social media platforms are targeted and what precisely that is. The discussion paper states that the intention is to target "major platforms" (discussion guide). However, the definition in the technical paper captures all social media platforms (see definitions of OCS and OCSP in paras 2 and 4). Europe's proposed *Digital Services Act* differentiates between "online platforms" and "very large online platforms" based on the number of users, imposing more onerous obligations on the large platforms. Under the Canadian proposal, the Governor in Council would have the power to add or remove categories of services from the definition of OCS. The Federal Government should consider carefully the OCSPs it wants to target. For example, <u>JustPaste.it</u> was started by a Polish student from his bedroom, and for a while, it was the platform of choice for ISIS. Justpaste.it has taken steps to address the challenge of terrorist content on its site, including joining the <u>Global Internet Forum to Counter Terrorism (GIFCT)</u>. Based on the technical paper, JustPaste.it would be captured as an OCSP, but if the intent is to target major platforms, then JustPaste.it would potentially be excluded from the scope. As will be evident, the proposal does not impose obligations on a sliding scale like the *Digital Services Act*. The platform is either in or out.

Despite the title 'online harms,' the proposal more narrowly targets criminal content, specifically terrorist content, content that incites violence, hate speech, non-consensual sharing of intimate images and child sexual exploitation content. Limiting the ambit to these five harms may be a surprise to the public, as a great deal of other harmful online activities such as bullying, harassment, defamation, or invasion of privacy are out of scope. There would be unavoidable constitutional questions if the bill were to include all of these harms and the kitchen sink, but as drafted, the proposal creates an odd situation where victims of great swaths of abuse and harm cannot avail themselves of the regulator. Not to let the perfect be the enemy of the good, the content that *is* covered by the proposal certainly should be (and is already addressed criminally), but there is enormous room for improvement if this proposal is going to live up to its name.

As an example, let's examine how narrow hate speech and terrorism are from a legal perspective. Hate speech as interpreted by the Supreme Court of Canada in *Saskatchewan (Human Rights Commission) v Whatcott*, 2013 SCC 11 (CanLII) (*Whatcott*), sets quite a high bar to meet: to qualify, content must communicate an expression of "detestation" or "vilification" of an individual or group on the basis of a prohibited ground of discrimination. Hurtful, humiliating, or offensive comments do not meet this threshold, even when based on a protected characteristic, such as religion, sexual orientation, gender identity or disability. Similarly, extreme, venomous abuse that isn't based on a protected characteristic while hate*ful* would not be hate *speech* (paras 41, 55-59). As one can readily observe, this leaves a tremendous grey area of abusive, arguably quite harmful content outside of the scope of this proposal.

Terrorist content is another example where many would say they have a general idea of what it includes but would struggle to produce a legal definition. Indeed, even the *Criminal Code* definition is spread across multiple sections, requiring some effort to pull together a clear understanding (see analysis of <u>Bill C-51</u> by Craig Forcese and Kent Roach <u>here</u>). The technical paper classifies terrorist content as that which both "actively encourages terrorism and which is likely to result in terrorism" (technical paper, s 8). It is difficult to gauge whether the definition of terrorist content in this proposal expands or mirrors that of the *Criminal Code*, in particular s 83.221 that criminalizes counselling another "to commit a terrorism offence without identifying a specific terrorism offence." This determination is also made more difficult by unanswered questions about whether platforms would be required to assess the criminality of the objectionable content on the criminal standard (beyond a reasonable doubt) or under a regulatory or civil standard (balance of probabilities).

Forcese and Roach warn that "any terrorist speech prosecution, especially for speech on the internet, will be difficult to sustain." (at 215) Examining a case where criminal charges were brought relating to 85 different social media posts from 14 different accounts, they identified the difficulties in assessing whether a given instance of speech amounts to "counselling" terrorism, especially when there is more of a cumulative effect than a clear black-and-white example. There was also concern that the judge may have been too focused on individual posts, and they suspect that "a criminal jury might ... have taken a more holistic approach", seeing the criminality in the forest where it was lacking in any individual tree (at 214). This is an equally pressing concern in the realm of content moderation, given that any individual piece of content lacks the context of other posts from the same user. While Forcese and Roach would support a separate form of terrorist speech offence not tied to the "counselling" offence found in the *Criminal Code* (s 83.221), we have to question whether this proposal seeks to introduce that very thing in a regulatory setting.

A danger that arises from these complex definitions is that a content moderator without legal training may resort to bias or heuristics rather than performing in-depth analysis of borderline cases where the decision to remove the content rests on a contextual analysis. Moderators are already overworked and not qualified to make legal determinations. Combining this with the virtual mountains of flagged content that they are tasked with assessing will inevitably lead to over-removal and inadequate consideration of the legal criteria. Empirical studies show a tendency by

platforms to over-remove content in notice and takedown regimes, meaning that legal content is already removed even without 24-hour time limits. This is exacerbated when automated mechanisms are used as the level of nuance and appreciation of context required to make these kinds of decisions is currently beyond their capability.

#### **Recommendations:**

- "Online Criminal Content Regulation" is a more accurate nomenclature until the proposal addresses other harmful content that doesn't rise to the level of the criminal definitions.
   "Beverage regulation" would not be an accurate name for a bill that only addressed alcoholic beverages.
- Consult and rescope the definitions of harmful content. In particular, examine the impact
  of adopting narrow definitions from the *Criminal Code* and related case law versus
  broader definitions in terms of the reality of content moderation practices, and harmful
  content sought to be reduced. The approach should be clear and justification provided.
- In evaluating harmful content, ensure that situations are captured where volume and persistence creates a situation of harm, even where any individual act or post would not violate the regulations.
- Introduce laddered obligations drawing from the *Digital Services Act*. There should be specific and more onerous obligations on major platforms, however defined, but other platforms should not be entirely out of scope.

#### Regulator

The proposal would create a Digital Safety Commission funded by fees levied upon industry. It would be comprised of three bodies: the Digital Safety Commissioner, Recourse Council, and Advisory Council. We broadly favour the idea of a new regulator, but it will depend on some of the finer details that are not set out in the proposal. The need to see the finer details of what is proposed is acute in this case because this will be a regulator of expression online, an unprecedented role for a regulatory body well beyond that of a human rights commission, which could have a potentially sweeping impact on day-to-day expression online. The scope and remit of the regulator needs to be fleshed out to ensure that it carefully balances rights, in particular expression, equality, and privacy, with a clear understanding of the platform economy. And like any regulatory entity, whether this is a good idea depends on the entity being suitably funded and populated with individuals with the right training and expertise.

The Digital Safety Commissioner would bear some resemblance to the role of our federal privacy commissioner. The Commissioner would oversee and enforce content moderation obligations and engage in education, research, and outreach (discussion guide, module 1, technical paper, module 1(a)). The Commissioner would receive and investigate complaints about non-compliance by regulated entities. Appeals of decisions of the Commissioner would be made to the Personal Information and Data Protection Tribunal (Tribunal), which is proposed to be created with <u>Bill C-11</u>, (An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts, 2<sup>nd</sup>

Sess, 43<sup>rd</sup> Parl, 2020) the proposed new consumer privacy legislation to replace the *Personal Information Protection and Electronic Documents Act*, <u>SC 2000, c 5</u> (see discussion <u>here</u>). The Commissioner would also have the power to do such things as proactively inspect for compliance or non-collaboration, issue reports and compliance orders.

Importantly, the Commissioner would have extraordinary power to recommend or refer noncompliance to bodies with the power to impose significant fines or order website blocking and filtering. For example, the Commissioner can recommend an administrative monetary penalty of up to 10 million dollars or 3% of gross global revenue, which would be decided by the Tribunal similarly charged with administering fines for privacy breaches. Or non-compliance could be referred to prosecutors with potential fines up to 25 million dollars or 5% of gross global revenue. Further, the Commissioner could apply to the Federal Court for an order that an ISP block or filter entire websites that repeatedly fail to remove child sexual exploitation or terrorist content (technical paper, paras 102-109). The immensity of these fines or recourse, coupled with the substance of the rules proposed, creates a high-risk environment that incentivizes over-removal of content by platforms to avoid legal risk.

The Digital Recourse Council, comprised of 3-5 members, would offer a different dispute resolution mechanism. While the Commissioner would focus on whether the platform has in place the procedural safeguards mandated by legislation, the Recourse Council would be concerned with whether a platform made the correct decision about a specific item of content. A person may make a complaint to the Recourse Council concerning a decision of a platform to either remove or not remove content. However, a complainant must first exhaust all avenues of appeal within the platform. Once a complaint is made, the platforms and affected individuals would be provided with a notice of the complaint and an opportunity to make representations. If the Council decides the content is harmful, they can order the OCSP to take it down. If the Council decides the content is *not* harmful, they will issue their decision to the OCSP, and it is then in the hands of the platform whether to reinstate or remove the content subject to the platform's own terms of use (technical paper, paras 45-59).

Hearings by the regulator (either Commissioner or Council) can be held in camera if there are compelling reasons to do so. The government suggests these reasons could include privacy, national security/defence, international relations, or confidential commercial interests (technical paper, para 59). These secret hearings have attracted a great deal of critical comment, and we suggest they need to set a clear threshold or criteria for situations where these can be invoked.

The Advisory Board would be comprised of up to 7 part-time members who would provide expert advice to both the Commissioner and Recourse Council about a variety of issues such as "emerging industry trends and technologies and content-moderation standards" (discussion paper, technical paper paras 71-75). Khoo recommends that the advisors are integrated within the Commissioner's office and Recourse Council. We are not necessarily opposed to a separate advisory council, but further consultation is required about the best structure for these three bodies. The concept of a digital regulator to address human rights or online harms issues is something that has been advocated by some scholars. Khoo recommends the creation of a centralized regulator to address technology-facilitated gender-based violence in her ground-breaking report "Deplatforming Misogyny." She envisions a body with a dual mandate to provide legal recourse and support to those impacted, and research and training. One of the authors of this post, Emily Laidlaw, has advocated for creation of a digital regulator in her scholarship. For example, the framework for a digital rights commission was detailed in chapter six of Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibilities, (Cambridge: Cambridge University Press, 2015), with similar emphasis to the Digital Safety Commission on the need for multiple forms of support in the form of a remedial mechanism, corporate support (policies, assessment tools, audits), and education and research. This framework was developed into a specific proposal for the Law Commission of Ontario for its project Defamation Law in the Internet Age. The crib notes version is that Laidlaw recommends creation of an online tribunal for defamation disputes modelled on British Columbia's Civil Resolution Tribunal (see here and here). Further, several states have created, or are in the midst of creating, regulators to address some aspects of online harms, including in the UK and Australia.

An exploration of the benefits and drawbacks of alternative regulators for online harms is beyond the scope of this blog post. In short, the high volume of content combined with the potential devastating harms and need for speed in addressing the complaint makes courts unsuitable to adjudicate most cases. Further consultation is necessary to ensure that the regulator is narrowly scoped and achieves the goal of reducing harm and protecting rights. Some questions include:

- How will the complaints process to the Recourse Council be structured to ensure access to justice and disincentivize frivolous or abusive complaints? Examples include issues of volume of complaints, specious complaints, ease of making complaints, disparate burdens being placed on complainant/complainee.
- Who can complain?
- What is the burden of proof?
- How will this process be structured to ensure speedy resolution and due process?
- How will a complainant prove that they have exhausted all avenues of appeal via the platform? How much additional time, burden and chilling effect will this place on a complainant whose content was incorrectly removed?
- What should be the training and expertise of the Recourse Council?
- How will grey zone expression be treated?
- How will the Recourse Council intersect with the internal content moderation policies of the OCSPs?
- How will the Advisory Council interact with the other bodies? For example, what if the Advisory Council's advice is repeatedly not accepted or adopted by the Recourse Council or Digital Commissioner?

#### **Recommendation:**

 Consultation on the details of the proposed Digital Rights Commission with a focus on fleshing out the scope and remit to ensure access to justice and balancing rights.

Stockness - construction of a construction of the state of the state of a construction by operation of the state of the

#### **Proactive Monitoring**

The technical paper obligates OCSPs to "take all reasonable measures, which can include the use of automated systems" to identify and remove harmful content (technical paper, para 10). To comply with this obligation necessitates that a platform pro-actively monitor content hosted on their services. This is because the burden is on the OCSP to identify harmful content for removal. Thus, the platform must come up with a way to find this content, which usually entails broad surveillance, often analyzed and actioned through automated means, and at risk of function creep. The impacts of such an approach are numerous, including the privacy and freedom of expression of users, often with a greater impact on marginalized and racialized groups. This can be contrasted with a complaints-based system, such as a <u>notice and action regime</u>, which relies on user complaints to trigger a platform's obligation to act.

General laws that mandate proactive monitoring are controversial and criticized as a human rights infringement, and for good reason. For example, David Kaye, the former Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, stated in his 2018 report that proactive monitoring and filtering are "inconsistent with the right to privacy and likely to amount to pre-publication censorship." (paras 15-17, 67) These risks are compounded when content is prevented from being uploaded, which operates as a system of prior restraint. It creates an opaque system for users and state bodies tasked with oversight, uncertain of the rules, process, or decision-making behind moderation decisions.

This is not to say that automated systems should never be used. That would be unrealistic, and the conversation is better directed to how these systems can be designed in a way that is human rights compliant. Further, this is not to say that platforms should never prevent content from being uploaded, in particular child sexual abuse content. However, no state should mandate a general obligation to monitor. Rather, the obligation, if any, must be more narrowly carved. The proposal states that such measures should be implemented in a way that does not discriminate pursuant to the *Canadian Human Rights Act*, <u>RSC 1985</u>, <u>c H-6</u> (technical paper, para 10). We are of the opinion that this cannot be solved at the implementation stage, and the provision must be scrapped or more narrowly carved.

There are certainly examples of legislation that impose proactive monitoring of some sort. Kaye <u>cites</u> both China's 2016 <u>Cybersecurity Law</u> and Germany's <u>Network Enforcement Act</u> (NetzDG) as laws that explicitly or implicitly force proactive monitoring that either lead to filtering or reporting to law enforcement (paras 15-16). However, Article 15 of the *E-Commerce Directive* prohibits European Member States from mandating general proactive monitoring, although specific content might be actioned to be removed and kept down. Further, the prohibition on general monitoring was maintained in the *Digital Services Act*, and exploration of such an obligation for terrorist content was softened in the final version of the EU's <u>Regulation on</u> preventing the dissemination of terrorist content online.

The UK's approach to proactive monitoring in the <u>Online Safety Bill</u> is illustrative as it is more narrowly circumscribed. There is no general obligation to monitor, although arguably the duty on platforms to take steps to manage the risk of harm of their platforms entails proactive monitoring. More specifically, the proposal is that the regulator Ofcom could issue a Use of Technology notice. The notice would only be available after a warning was provided and would be limited to child sexual abuse material and terrorist content, and the notice would mandate the use of "accredited technology" selected by Ofcom. We are not weighing into the strengths and weakness of the UK approach here, which is also controversial, but rather aim to highlight that even compared to the highly contentious UK model, the Canadian proposal is an outlier.

#### **Recommendation:**

- The proposal of a general obligation to monitor all harmful content should be categorically rejected. Consultation and analysis should be undertaken to explore options that are proportionate and effective to achieve the objective of reducing circulation of harmful content. Options include, without endorsement, but for discussion, more targeted measures:
  - A duty of care model requiring platforms take reasonable care in the management of their services with specific safeguards to address the risk of general monitoring;
  - Exploration of human rights safeguards that can be the central framework in content regulation and what that would entail e.g., criteria for specific versus general monitoring; and
  - Exploration of what a system of reasonable decision making might be, and how to build a cushioning system for mistakes (see this proposal by <u>Marcelo Thompson</u>).

#### 24 Hour Takedown Requirements

An aspect of the proposal that has already attracted a great deal of critical attention is the requirement for content to be addressed by a platform within 24 hours of being flagged. This 24-hour requirement is separate from a platform's obligations to take all reasonable proactive measures, but instead starts a clock from the point at which a piece of content is flagged. The Governor in Council may pass regulations to adjust this timeframe for different types or subtypes of harmful content, but under this power the timeline could also be *shortened* below 24 hours (technical paper, paras 11-12).

From the point at which the content is flagged, the platform has 24 hours to either remove the content or respond to the flagger indicating that the content does not meet the definition of harmful under the Act. It is worth bearing in mind that a platform like Facebook already has systems to flag content that goes well beyond the scope of harmful content captured in this proposal. This context is needed when considering the scale and volume of content that must be moderated. A report from NYU indicates that for Facebook alone, they made moderation decisions on approximately 3.75 billion pieces of content in the first quarter of 2020, and the accuracy of those decisions falls well short of 100%. As acknowledged by Facebook founder and CEO Mark

Zuckerberg: "[t]he vast majority of mistakes we make are due to errors enforcing the nuances of our policies rather than disagreements about what those policies should actually be. Today, depending on the type of content, our review teams make the wrong call in more than 1 out of every 10 cases." (source) The NYU report goes on to recommend that Facebook double the size of its moderation team just to tackle the accuracy deficits in their existing moderation regime. Imposing a 24-hour window for reviewing and responding to specific types of content – especially if Facebook chooses not to double its moderation staff – would suggest that concerns over the quality of moderation decisions will only increase.

The proposal seems modelled on German legislation known colloquially as NetzDG, which also imposes a 24-hour time limit to remove content. However, even NetzDG, controversial in its own right, appreciates that decisions about the illegality of content sometimes require more than a few moments to make. NetzDG restricts the 24-hour rule to obviously illegal content and allows for up to a week for a platform to respond to content in circumstances where factual considerations could render the content legal, or where the poster might have a legitimate defence for posting it. Thus, NetzDG grants platforms more time to assess expression in the grey area. Canada's proposal contains none of that nuance.

This consideration of nuance is even more important here given that hate speech must be assessed in light of the Supreme Court of Canada's jurisprudence (e.g. *Whatcott, R v Keegstra*, [1990] 3 <u>SCR 697, 1990 CanLII 24</u>). As the NYU report highlights, the moderators for Facebook are not legally trained, and are frequently outsourced to other countries. Expecting accurate analysis of hate speech by untrained and overworked moderators is unrealistic and even less so with a liability clock ticking in the background. When the incentives on a platform weigh almost entirely in favour of removal in situations where there is the slightest doubt, and they have no reasonable motivation to consider the poster's right to free expression, the inevitable outcome is censorship.

Let us be entirely clear here – removal is the right decision for legitimately harmful content, and it is important that such content is removed quickly. The danger is that there remains a significant grey area within which entirely legal content could be removed solely due to platform riskavoidance. The question the proposal wrestles with - as do all of us working in this area - is where to draw the line, and it is our view the proposal heavily errs on the side of protection from harm in a way that undermines their goals. It is notable that both the discussion and technical papers devote minimal attention to the value of freedom of expression. The 24-hour rule embodies the unbalanced analysis threaded throughout the proposal. Further, this proposal would disproportionately impact marginalized, racialized and intersectional groups (see Suzie Dunn's commentary here). For example, platforms' internal complaints systems are regularly used as mechanisms of abuse whether by a persistent individual or mobs who maliciously flag content, or because the design of the content moderation system and its practice discriminates. The examples are endless: removal of Black Lives Matters posts, LGBTQ+ posts, sexualized content and posts raising awareness of missing and murdered Indigenous women and girls (see, scholarship on this issue here and here). The result is that the voices of the very groups we seek to protect would be further silenced.

### **Recommendations:**

- The 24-hour time limit should be abandoned in favour of a generic obligation to act expeditiously. Or, at minimum, exceptions should be drafted, which allow additional time to engage in a contextual analysis of expression in the grey zone, similar to the NetzDG model.
- Incentivize platforms to protect free expression when making moderation decisions in order to avoid banket removals. Consider addressing the prevalence of harmful content, not merely its presence (see <u>Facebook Whitepaper</u> at pp 9 & 13).
- Explore more creative options. For example, the *Digital Services Act* incorporates a "trusted flagger" system wherein complaints from a verified trusted flagger (person or organization) can be handled on an expedited basis. The status of the trusted flagger is contingent on the accuracy and quality of complaints made. If a trusted flagger has a certain number of "false positives" they can lose their status. (Article 19(5)-(6))

## Website Blocking

In a section of the technical paper under the heading "Exceptional Recourse" are provisions dealing with granting powers to the Digital Safety Commissioner to block entire websites (paras 120-123). On its face, this seems to be an alarming power of censorship, but as drafted it would have quite narrow application. Website blocking would be restricted to child sexual exploitation content and terrorist content. Further, before this could be used, a provider must have demonstrated persistent non-compliance with orders to remove such content, *and* all other enforcement measures must have been exhausted. To reach the point of website blocking, there would have to be compliance orders made, fines issued, which may also be preceded by hearings, and each of these decisions can also be appealed before resorting to banishing a website from Canadian soil.

In the UK, for example, their proposed *Online Safety Bill* would permit the regulator, Ofcom, to enact "business disruption measures", an escalating form of sanction against non-compliant services. The measures would actually apply to ancillary parties rather than the targeted service directly, meaning ISPs, app stores, payment providers or search engines. The UK Bill frames these as levers to be used against platforms that are bucking the regulator's authority, allowing Ofcom to cut off payment processing and search results for the misbehaving service before proceeding to outright blocking. Notably, the business disruption measures can be used for various forms of non-compliance and are not strictly limited to persistent non-removal of terrorist or CSEA content.

One of the main issues with website blocking is overreach and overbreadth. The proposal here would allow the blocking of entire platforms. When website blocking has been used in a more targeted and human rights compliant manner, it has either blocked specific webpages or targeted websites that are primarily devoted to hosting illegal content (e.g. piracy websites). The proposal here does not limit website blocking in this way; rather, it relies purely on the idea of blocking as a last resort.

## **Recommendations:**

- Maintain tightly limited scope and availability of this enforcement measure, including requiring judicial authorization.
- Add warning steps and procedural protections to ensure platforms can make representations before drastic measures are pursued.
- Examine limiting website blocking to specific webpages, or when that is not possible, to OCS that are primarily devoted to sharing illegal content.

## Mandatory Reporting

The discussion paper proposes two options for consideration. First, mandatory reporting to law enforcement where "there are reasonable grounds to suspect there is an imminent risk of serious harm." (Module 2) This is a reasonable and high threshold to trigger reporting to police and something which some major platforms already do (see, for example, <u>Twitter</u>). The second option proposes a significantly lower threshold. It would mandate reporting to law enforcement (criminal content) and CSIS (national security content) when there are reasonable grounds to believe or be suspicious that the content is illegal within the five categories of content. This is not a good approach. It would force a platform to report content that *might* be illegal, thus targeting grey zone speech. As identified above, Black Lives Matter posts have been mistakenly labelled hate speech and removed in the content moderation process. Pursuant to this proposal, such posts would need to be forwarded to law enforcement, further harming racialized groups and undermining equality-seeking goals of online harms legislation. As Daphne Keller <u>notes</u>, Germany has made a similar proposal, which is being <u>challenged</u> by Google for violating fundamental rights. If the first option is implemented, it is critical that mandatory reporting is not coupled with a proactive monitoring obligation.

## **Recommendations:**

- Limit mandatory reporting to circumstances where it is reasonably suspected there is an imminent risk of serious harm.
- Limit the basis for mandatory reporting, to a complaints-based approach or reasonable awareness.
- Do not impose proactive monitoring coupled with any mandatory reporting.

## **Transparency Obligations**

To aid in monitoring and enforcing the various aspects of the proposed regulation, OCSPs will also be subject to reporting and transparency requirements (technical paper, para 14). Some of these are designed to provide insight into how moderation is being conducted behind closed doors, and others are a somewhat roundabout way of pressing platforms to address systemic concerns.

Platforms will provide data on an annual basis detailing the types and volumes of harmful content found, and separately disclosing content deemed objectionable on the basis of the platforms' own community standards, but which would not have been defined harmful under the regulations. They are also required to report on the resources and personnel allocated to content moderation, along with their procedures, practices, and systems, including automation. Further, the proposal requires that platforms collect and sort data in a way that might be difficult to achieve. For example, the proposal would require Canada-specific data, which depending on the platform, may not be realistic to provide. For example, would the data about the "volume and type of content dealt with at each step of the content moderation process" (technical paper, para 14) be limited to posts made by Canadian-based users, or visible by Canadian users? Would any public posts visible by a Canadian be in scope?

The proposal would also require platforms to report on how they monetize harmful content, which stands out from the others as an odd inclusion. It seems designed as a form of public shaming to these companies, and therefore the data would be less reliable from the start, given that companies have an incentive to claim that they are not profiting from the hate speech or child pornography posts of their users. Also, the impetus behind this reporting requirement seems to be inspired by the EU's proposed *Digital Services Act*, wherein platforms are obliged to perform a yearly risk assessment to identify systemic risks arising from their services. However, the Federal Government's proposal is flawed because it frames the platforms as villains being unmasked by the data, rather than using the European approach enlisting platforms as collaborators seeking to solve the systemic problems.

Mandating and standardizing the content and requirements around transparency for platforms is essential, both as a method of accountability and as an avenue to better understand and address systemic problems.

#### **Recommendations:**

- Platforms should still be required to address systemic problems, but the proposal should avoid framing the requirement as a "gotcha" on platforms, rather enlisting platforms as collaborators, and using data from transparency reports as an accountability tool.
- Consult with platforms and organizations such as GIFCT and the <u>Global Network</u> <u>Initiative</u> about appropriate and achievable transparency reporting requirements.

#### Conclusion

Overall, while there are meritorious elements to the Federal Government's online harms proposal, the problematic areas are *very* problematic. We commend the proposal to create a Digital Safety Commission. However, the substance of the rules, although ticking all the right boxes as to topics that should be on the agenda for debate, requires a massive overhaul. When we say that it ticks the right boxes, we mean that it explores key issues of debate in internet law and policy, such as website blocking, time-limited content takedown rules, identification and actioning of content, transparency reporting and so on. However, with each of these topics, the solution proposed is rather blunt when nuance is needed to balance the various interests and rights. In the area of content regulation, to achieve the objective of an internet ecosystem that broadly strives to protect and balance various rights and interests, it is the multitude of little decisions that determine the overall effect.

Canada needs legislation to address online harms, but there must be more thorough consultation and more thoughtful consideration of every element of this proposal. There are multiple other regimes to look to that have tackled some of these very same issues. None are perfect, but the EU's *Digital Services Act* would be a good place to start, and the wealth of scholarly, industry and civil society attention that has been devoted to the issue of platform regulation and content moderation.

#### **Summary of Recommendations:**

- "Online Criminal Content Regulation" is a more accurate nomenclature until the proposal addresses other harmful content that doesn't rise to the level of the criminal definitions.
   "Beverage regulation" would not be an accurate name for a bill that only addressed alcoholic beverages.
- Consult and rescope the definitions of harmful content. In particular, examine the impact of adopting narrow definitions from the *Criminal Code* and related case law versus broader definitions in terms of the reality of content moderation practices and harmful content sought to be reduced. The approach should be clear and justification provided.
- In evaluating harmful content, ensure that situations are captured where volume and persistence creates a situation of harm, even where any individual act or post would not violate the regulations.
- Introduce laddered obligations drawing from the *Digital Services Act*. There should be specific and more onerous obligations on major platforms, however defined, but other platforms should not be entirely out of scope.
- Consultation on the details of the proposed Digital Rights Commission with a focus on how to structure it to balance rights and ensure access to justice.
- The proposal of a general obligation to monitor all harmful content should be categorically rejected. Consultation should be undertaken to explore options that are proportionate and effective to achieve the objective of reducing circulation of harmful content. Options include, without endorsement, but for discussion, more targeted measures:
  - A duty of care model requiring platforms take reasonable care in the management of their services with specific safeguards to address the risk of general monitoring;
  - Exploration of human rights safeguards that can be the central framework in content regulation and what that would entail e.g. criteria for specific versus general monitoring;
  - Exploration of what a system of reasonable decision making might be, and how to build a cushioning system for mistakes (see <u>Marcelo Thompson</u> for this proposal).
  - The 24-hour time limit should be abandoned in favour of a generic obligation to act expeditiously. Or, at minimum, exceptions should be drafted, which allow additional time to engage in a contextual analysis of expression in the grey zone, similar to the NetzDG model.
  - Incentivize platforms to protect free expression when making moderation decisions in order to avoid banket removals. Consider addressing the prevalence of harmful content, not merely its presence (see <u>Facebook Whitepaper</u> at pp 9 & 13).

- Explore more creative options. For example, the <u>Digital Services Act</u> incorporates a
   "trusted flagger" system wherein complaints from a verified trusted flagger (person or
   organization) can be handled on an expedited basis. The status of the trusted flagger is
   contingent on the accuracy and quality of complaints made. If a trusted flagger has a
   certain number of "false positives" they can lose their status. (Article 19(5)-(6))
- Maintain tightly limited scope and availability of this enforcement measure, including requiring judicial authorization.
- Add warning steps and procedural protections to ensure platforms can make representations before drastic measures are pursued.
- Examine limiting website blocking to specific webpages, or when that is not possible, to OCS that are primarily devoted to sharing illegal content.
- Limit mandatory reporting to circumstances where it is reasonably suspected there is an imminent risk of serious harm.
- Limit the basis for mandatory reporting, to a complaints-based approach or reasonable awareness.
  - Do not impose proactive monitoring coupled with any mandatory reporting.
  - Platforms should still be required to address systemic problems, but the proposal should avoid framing the requirement as a "gotcha" on platforms, rather enlisting Platforms as collaborators, and using data from transparency reports as an accountability tool.
- Consult with platforms and organizations such as <u>GIFCT</u> and the <u>Global Network</u> <u>Initiative</u> about appropriate and achievable transparency reporting requirements.

This post may be cited as: Darryl Carmichael and Emily Laidlaw, "The Federal Government's Proposal to Address Online Harms: Explanation and Critique" (September 13, 2021), online: ABlawg, http://ablawg.ca/wpcontent/uploads/2021/09/Blog\_DC\_EL\_Federal\_Online\_Harms\_Proposal.pdf

To subscribe to ABlawg by email or RSS feed, please go to http://ablawg.ca

Follow us on Twitter @ABlawg



#### Consultation on Proposed Approach to Address Harmful Content Online

#### Submission by Dr. Natasha Tusikov (York University, <u>ntusikov@yorku.ca</u>) and Dr. Blayne Haggart (Brock University, <u>bhaggart@brocku.ca</u>),

#### 24 September 2021

We are writing this submission in our capacity of academics who have researched and written extensively in the areas of platform and internet regulation.

Natasha Tusikov is an Assistant Professor of Criminology at York University. Her book, *Chokepoints: Global Private Regulation on the Internet*, deals directly with internet companies' efforts to police illegal and harmful content and activities by their users. She is a research fellow with the Justice and Technoscience Lab (JusTech Lab), School of Regulation and Global Governance (RegNet) at the Australian National University. She has also published scholarly research and opeds in the areas of internet governance, the Internet of Things, smart cities and data governance, and regulating hate speech on social media. Before obtaining her PhD at the Australian National University, she was a strategic criminal intelligence analyst and researcher at the Royal Canadian Mounted Police in Ottawa.

Blayne Haggart is an Associate Professor of Political Science at Brock University and a Senior Fellow with the Centre for International Governance Innovation (CIGI). He is the author most recently of "Democratic Legitimacy in Platform Governance" (*Telecommunications Policy* 45, no. 6 (2021), with Clara Iglesias Keller) and "Global platform governance and the internet-governance impossibility theorem" (*Journal of Digital Media & Policy* 11, no. 3 (2020)).

Together we are co-editors (with Prof. Jan Aart Scholte) of the 2021 edited volume, *Power and Authority in Internet Governance: Return of the State?* (Routledge). We have also published several opeds on the regulation of the digital sphere in *The Toronto Star, The Globe and Mail, The Conversation* and through the Centre for International Governance Innovation.

We are strongly in favour of government regulation of internet intermediaries and the goal of creating an online environment that is more conducive to socially healthy exchanges. The primary issue when it comes to internet intermediaries is not, should they be regulated by government, but *how* should government regulate them. However, we have significant substantive and procedural concerns with the government's proposed approach to address harmful content online. In this note we highlight four in particular:

- 1. The presentation of a detailed *fait accompli* before engaging in meaningful, substantive public consultations;
- 2. The lack of evidence presented explaining and justifying these particular interventions;
- 3. Its ineffectiveness in addressing fundamental structural problems with social media that give rise to the problems the government says it wants to address.
- 4. The focus on regulating social media companies overlooks the necessity of regulating the broader digital economy, including online marketplaces and the financial technology industry.

Based on these concerns, which we outline below, we call on the government:

- To undertake substantive, open consultations to determine how Canada should address these and other related issues.
- 2. To present research and evidence outlining the problems being addressed and justifying the government's chosen approach.
- 3. To pursue a regulatory framework that involves structural reforms to address incentives baked into social media companies' advertising-dependent and data-fuelled business models.
- To consider deep institutional reforms to regulate the digital economy, including regulation to address monopolistic behaviour and institutional reforms to strengthen and promote in-house digital policymaking expertise.

We address each of these in turn.

#### 1) Lack of consultation

Most fundamentally, the government has presented Canadians with a whole-cloth policy proposal without first engaging in consultations with Canadians to determine the best way to proceed with regulating online illegal content. This approach is not in keeping with best practices in government policymaking. Instead, it is obvious that the government has looked to other countries for ideas about what we should do here. For example, the requirement that internet intermediaries make content found to be harmful/illegal inaccessible within 24 hours is clearly borrowed from the German NetzDG regime, while the exclusive focus on illegal content (terrorist content, content that incites violence, hate speech, revenge porn and child sexual exploitation) seems to reflect critiques that the UK Online Harms legislation's focus on illegal *and harmful* speech may unnecessarily stifle legal (if distasteful) speech.

While one of the advantages of being a laggard when it comes to online intermediary regulation is that we can learn from the experiences of other countries, such policies need to be considered and justified in the Canadian context. This includes considering how we could improve on other countries' experiences. Internet intermediary regulation, and regulation generally, is not a matter of plug-and-play.

By presenting Canadians with the answer rather than the question, the government is pre-empting the necessary conversation over how these companies should be regulated.

We also note that both the German and UK approaches, which have so obviously inspired the Canadian proposal, were themselves the outcomes of extensive consultative and legislative processes. In particular, the UK Online Safety Bill currently before the UK Parliament was the product of years of consultations beginning in 2017, including a White Paper. The consultation process for the Online Harms White Paper (document here), for example, consisted of 19 questions, including several openended ones.

One of the upsides of the UK's extensive consultations and reporting is that although opposition to it exists (and will continue to exist), nobody can say they've been taken by surprise by the resulting legislation, or that it hasn't been properly considered. Conversely, one of the major downsides of the Canadian proposal is that it reads like a hastily assembled grab-bag of ideas that other countries have implemented, rather than something that has been subject to sound vetting by policy experts and interested Canadians.

Internet intermediaries need to be regulated by government. However, it's not enough just to do something; we also need to get the legislation right. This requires a much more open and thoughtful process than what the government has put in place. Rather than start with one specific, intricate solution, Canadians and the government need to start with the issue itself, and various options, before settling on one. The UK Online Harms consultation process provides one model in this regard. Another, as we discuss in the context of smart-city regulation, is Brazil's two-step consultation process leading to its pathbreaking internet bill of rights legislation (*Marco Civil*): Hold consultations designed as a structured conversation addressing issues of concern; *then* consult on a specific draft plan.

#### **Recommendation 1**

That the federal government scrap the current proposal and engage in actual, two-step consultations with Canadians to address online internet intermediaries' socially harmful behaviours.

#### 2) Lack of evidence presented

Neither the government's Discussion Guide nor its Technical paper contain any contextual information or links to research that would allow an interested Canadian or non-expert to understand the nature of the problems being regulated or the implications of the government's proposed solution. Instead, these documents offer only a highly detailed, legalistic description of several interlocking processes and policies whose implications will be lost on anyone without a deep, technical understanding of the machinery of government and a pre-existing knowledge of the issue areas in question. There is nothing in here to educate Canadians regarding the policies and issues at play.

For example, child sexual exploitation is obviously anathema to any society. However, neither the Discussion Guide nor the government's Technical Paper contain any information contextualizing either the problem or the proposed solution. Most obviously, the possession and distribution of child sexual abuse images are already illegal. Internet intermediaries already do not allow this material on their services. What is the extent of this problem on, say, Facebook? Our point isn't that the existence of this illegal content on Facebook isn't a problem – it very may well be, and if it is, the government should definitely take action. Rather, it is to highlight that both documents fail to even discuss the scope of the problems and how they relate to internet intermediaries. Nothing has been presented to Canadians to justify why these particular issues have been selected and packaged together, and why this particular approach has been proposed. We address some of what's not covered in this proposal in Points 3 and 4.

The <u>UK Online Harms White Paper</u> offers a sobering contrast to the informational wasteland the government is offering Canadians. It is replete with links to surveys, examples, and other reports – to evidence – contextualizing and justifying its decisions. To its credit, it also indicates (as in Box 29 discussing AI and hate speech) where they still lack a full understanding of the issues and require more research. Nothing in the two documents the government is presenting to Canadians, meanwhile, even tries to justify the government's response. These are not discussion documents; they're legislative bullet points that have the practical effect of shutting most Canadians out of this important discussion.

Again, we point to both the UK Online Harms and the Brazilian *Marco Civil* policy processes as examples for the government to follow. Unlike the Canadian case, both processes were designed to

educate citizens about the issues (Brazil's case explicitly so), not just to present a detailed solution from on high.

No matter how serious the problems being addressed, you still have to explain your proposals. In this case, the government has not even attempted to do so. If the government is interested in pursuing sound, effective, evidence-based internet-regulation policy, it must explain the problem and justify its proposal.

#### **Recommendation 2**

That, as part of a revamped consultation process, the government present to Canadians properly researched explanations and justifications explaining the nature of the problems being addressed and why these specific solutions are being proposed.

#### 3) Inadequate consideration of fundamental structural problems

The government's discussion paper proposes to impose an obligation on regulated entities to monitor their systems for the categories of harmful content, including by establishing flagging, notice, and appeal systems and using automated systems.

This approach effectively asks social media companies to continue their already existing flagging programs. Moreover, these programs are too-often troubled by significant problems with <u>inaccurate or abusive flagging</u>, or are unduly <u>reliant on users</u>' policing problematic content. The discussion paper also seems to assume that the imposition of fines will encourage platforms to remove problematic content. However, these global companies have shrugged off massive fines in the <u>United States</u> and <u>Europe</u>.

The core problem with this approach is that calling for more flagging systems simply feeds into these companies' existing reliance on automation and their preference for self-regulation, which are central features of social media companies' business model. Social media companies minimize costs by automating many activities, and <u>outsourcing the human component</u> of their content-moderation systems to low-paid, often foreign, workers, a pattern similar to the labour offshoring that countless industries have engaged in for decades.

Regulation of social media — indeed, regulation of any online content and services — must begin with an understanding of the business models and, more broadly, the assumptions underlying the digital economy. Social media companies, which make most of their money via advertising, have business models designed to maximize user engagement and to promote viral content. Given their commercial reliance on user engagement as a growth metric, companies are often reluctant to enact measures that deal with bad actors, such as ridding their systems of <u>bots and fake accounts</u>, or setting rules that may limit viral content. Spreading harmful content can be a profitable activity for both <u>platforms</u> and <u>users</u>. During the pandemic, people have profited from pushing <u>fake cures</u> and <u>medical conspiracy</u> theories.

To address this structural problem, there must be structural reforms to social media companies' business models. In short, governments must consider reforming advertising as a revenue source, with the goal of minimizing social media companies' reliance on user engagement as a growth metric. Advertising is not the only way that a company can make money. Companies could generate revenues from subscriptions like Netflix or governments could provide funding in the form of <u>nationalizing</u> social media services as <u>public goods</u>. Governments could also get more involved in regulating social media companies'

algorithms so that they respond to democratically determined priorities, rather than reflecting the profitdriven motives of foreign companies.

#### **Recommendation 3**

## Regulation must entail structural reforms to address and counter negative incentives baked into social media companies' advertising-dependent and data-fuelled business models.

#### 4) Broader regulation of the digital economy

When it comes to platform regulation, a disproportionate amount of scholarly and public debate focuses on a few social media companies. Along with legislation that addresses the problematic business models of social media companies, the government needs to consider effective regulation of other areas of the digital economy such as competition policy and consumer welfare.

Government action to limit monopolistic online companies is vitally important because of the sheer scope and power of the handful of mostly American companies that dominate the provision of services online. Amazon, in particular, raises <u>monopoly concerns</u> in its dual role as marketplace operator and merchant. As an operator, Amazon is in an unrivalled position to privilege its products and control prices, while as a merchant, it can siphon data from its business rivals to create and push its Amazon-branded products. Similar problems of anti-competitive behaviour are evident in Apple and Google's <u>duopoly</u> of mobile operating systems and <u>app stores</u>.

One solution to this monopoly problem is a structural separation that would prohibit dominant actors from directly competing with the businesses reliant on their services. Structural separation would not allow search engines, social media, app stores or marketplaces to operate those services and compete directly with third-party businesses reliant upon those services, as is being proposed now in the United States in a <u>suite</u> of antitrust bills.

Another digital sector in vital need of reform are online payment providers. As Dr. Tusikov has <u>argued</u> <u>elsewhere</u>, given the concentration of the online payment industry, payment providers wield significant power to determine what content and services they approve for payment, in what can be called "<u>revenue</u> <u>chokepoints</u>." Payment providers exert a form of what international political economy scholar <u>Susan</u> <u>Strange</u> called "structural power": the ability to set the rules under which others operate. Payment providers' structural power is evident in their decade-long <u>war on sex</u> on the internet in which payment providers, especially those headquartered in the United States and with global operations, have a pattern of denying financial services to people and businesses involved in publishing legal sexual content.

Alongside monopoly problems in the digital economy is the growing role of technology companies such as Apple and Google providing financial services (i.e., fintech), as well as the increasing popularity of cryptocurrencies. To reign in this structural power and to provide effective regulation over the rapidly evolving financial technology (ie., fintech) sector, Canada could follow the lead of the Australian government. Australia has undertaken a <u>parliamentary review</u> of mobile payments and digital wallet services, and a Treasury-<u>commissioned review</u> (the so-called Farrell Report) of the payment system.

One of the <u>Farrell Report's</u> key recommendations, among those to strengthen licensing and competition requirements, tackles directly another key issue in digital economic governance: platform

exceptionalism. Platform exceptionalism contends that services delivered online or via an app should be treated differently than the same services delivered offline (for example, Uber and taxis, or Airbnb and hotels). The Farrell Report calls on Australian regulators to set rules based on the nature of the service, not on the entity providing the service. Under this rule, platforms providing payment services would not be treated differently than traditional financial institutions offering the same services. Simply put, the claim of "platform" would no longer be a perceived or actual regulatory advantage.

As we set out in a <u>three-part series</u> on regulating the online economy for the Centre for International Governance Innovation, what's needed is a concerted, institutional response to consider deep institutional reforms to regulate the digital economy in the Canadian public's interest.

We have two suggestions. First, create a successor to the <u>Economic Council of Canada</u> to provide inhouse advice to the government of the day on novel economic and social issues. Elsewhere, <u>we</u> and others, chiefly <u>Jim Balsillie</u>, founder and chair of the Centre for International Governance Innovation, have called for such a governmental institute focused on applied policy issues, including the economic and social challenges of a digital/datafied society. The government needs highly qualified, expert inhouse analysts to help set policy and evaluate outside advice with an eye to promoting policy in the national interest.

Second, and more importantly, the next government needs to reinvigorate its own bureaucracy to deal with the challenges of the twenty-first century. They could start by reforming or replacing the Competition Bureau, and its enabling laws, with an agency and legislative framework modelled on the <u>Australian Competition and Consumer Commission (ACCC)</u>. The ACCC has been at the forefront of mid-sized countries' attempts to regulate the digital economy, including social media companies. Canada also hasn't had a dedicated consumer protection agency or industry for decades now — another point we can borrow from the ACCC.

#### **Recommendation 4**

The government needs to consider deep institutional reforms to the digital economy, including regulation to address monopolistic behaviour and institutional reforms to strengthen and promote in-house digital policymaking expertise.

Secarity and a second second second prosecarity and second second second protraining and second second protraining and second second prosecond second second second prosecond second second second prosecond second second



ST. JOHN'S STATUS O WOMEN COUNCI

To: Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St Gatineau QC K1A 0S5 pch.icn-dci.pch@canada.ca

From: Safe Harbour Outreach Project 170 Cashin Avenue Extension St. John's NL A1E 3B6

To Whom It May Concern in the Department of Canadian Heritage,

Safe Harbour Outreach Project (known as SHOP), a program of the St. John's Status of Women Council and Women's Centre, advocates for the rights of sex workers in Newfoundland and Labrador. As an organization concerned with the safety and dignity of sex workers in Canada, we are concerned about the government's proposed initiative regarding digital harms. We are not alone in these concerns<sup>1</sup>.

Our community is deeply familiar with the kinds of harms that can be inflicted through the nonconsensual production and distribution of sexual media or sexual abuse materials, or other forms of online harassment. We are also deeply familiar with the additional harms that are created when the proposed 'solutions' to these issues do not centre the knowledge and expertise of sex workers themselves. Several elements of the proposed framework are cause for extreme caution.

- The 24-hour response and take-down requirement based on user claims is unrealistic, has no existing precedent in online spaces, and is more onerous than what even most local law enforcement can respond to when reports of harassment or illegal online content get reported. This will encourage websites to simply ban people and accounts outright across broad categories of sexual speech. Combined with the requirement to engage in proactive monitoring, this will result in harmful censorship. Such censorship is not distributed evenly: both human and automated flagging and filtering systems are unable to detect truly harmful or illegal content with accuracy<sup>2</sup>. Historically, these kinds of measures have disproportionately harmed sex workers<sup>3</sup>, 2SLGBTQ+ folks<sup>4,5</sup>, sex educators<sup>6</sup>, and other marginalized communities<sup>7</sup>.
- Both the takedown and monitoring requirements are especially burdensome to smaller independent platforms who do not have the necessary resources to accomplish such strict moderation timelines. Any regulations that burden independent entities in this way encourage the establishment of oligopolies, and discourage the kind of autonomous working environments

<sup>&</sup>lt;sup>1</sup> https://techpolicy.press/five-big-problems-with-canadas-proposed-regulatory-framework-for-harmful-online-content/

<sup>&</sup>lt;sup>2</sup> https://mitpress.mit.edu/books/nsfw

<sup>&</sup>lt;sup>3</sup> https://hackinghustling.org/posting-into-the-void-content-moderation/

<sup>&</sup>lt;sup>4</sup> https://eu.boell.org/sites/default/files/2021-06/HBS-e-paper-state-platform-moderation-for-LGBTQI-200621\_FINAL.pdf

<sup>&</sup>lt;sup>5</sup>https://www.washingtonpost.com/technology/2019/08/14/youtube-discriminates-against-lgbt-content-by-unfairly-culling-it-suit-alleges/

<sup>&</sup>lt;sup>6</sup> https://www.theatlantic.com/health/archive/2015/03/when-social-media-censors-sex-education/385576/

<sup>&</sup>lt;sup>7</sup> https://www.scientificamerican.com/article/the-harm-that-data-do/

that sex workers use to exercise more agency and self-determination in their careers environments and strategies that are inherently about safety for individuals.

- The requirements to maintain information and records about those suspected of committing a violation and to alert law enforcement before it is deemed that an illegal act has genuinely occurred are also very alarming. This will lead to the mass reporting of many innocent people, especially innocent people who are already demonized and criminalized for their gender expression, race, sexuality, and real or imagined involvement in sex work. The result will be a mass chilling of free speech, major infringements on privacy, and the devastating disruption of many lives. In the words of Daphne Keller, director on Program on Platform Regulation at Stanford's Cyber Policy Center, and formerly the Director of Intermediary Liability at CIS: "The human rights consequences of this privatized surveillance are sure to fall disproportionately on less powerful groups in society. We have every reason to expect people of color and other marginalized or vulnerable groups to face more suspicion, be reported to police more, and be mistreated more after that happens."<sup>8</sup> This is especially concerning given how the proposed framework extends extremely broad authority to the regulatory body without oversights in place to prevent these kinds of gross abuses of power.
- Finally, the provision that entire site ISPs may be blocked is very worrisome. This will enable discriminatory censorship of sites that are crucial for sex workers safety. Evidence demonstrates that limitations on access to online platforms in fact create the very conditions where people are more likely to be targeted for violence and exploitation<sup>9</sup>. For example, sex workers have faced increased violence and precarity since the removal of Backpage.com for supposedly harbouring harmful sex trafficking information<sup>10</sup>. This case was just deemed a mistrial precisely because prosecutors falsely and repeatedly suggested the site facilitated sex trafficking and child sexual abuse, rather than consensual adult sex work<sup>11</sup>. Similar mischaracterizations of internet platforms have occurred<sup>12</sup> and will lead to more harms against sex workers, without accomplishing the goal of reducing sex trafficking and child sexual abuse<sup>13,14</sup>.

Digital harms are a serious concern, but we must be extremely cautious to avoid generating new egregious and discriminatory harms through attempts to address that concern. The proposed Digital Harms framework has grave potential to hurt sex workers, 2SLGBTQ+ folks, BIPOC communities, and other marginalized populations. We implore the Canadian Government to reconsider these measures and to heed the experiences and expertise of these communities in drafting safe and effective alternatives.

Thank you for your consideration,

SHOP

<sup>&</sup>lt;sup>8</sup> https://techpolicy.press/five-big-problems-with-canadas-proposed-regulatory-framework-for-harmful-online-content/ 9 https://www.mdpi.com/2076-0760/10/2/58

<sup>10</sup> https://hackinghustling.org/erased-the-impact-of-fosta-sesta-2020/

<sup>11</sup> https://reason.com/2021/09/14/biased-testimony-in-backpage-trial-triggers-more-calls-for-a-mistrial/

<sup>12</sup> https://www.thedailybeast.com/facebook-a-hotbed-of-child-sexual-abuse-material-with-203-million-reports-far-more-than-pornhub

<sup>13</sup> https://www.businessinsider.com/fosta-sesta-anti-sex-trafficking-law-has-been-failure-opinion-2019-7

<sup>14</sup> https://newrepublic.com/article/162823/sex-trafficking-sex-work-sesta-fosta

Machaella, and Sachaella, and Anthread Articles, and Articles and Anthread Machaella, Anthread Anth

## Felicia Mazzarello

From: Sent: To: Subject: Rose < s.19(1) September 24, 2021 8:03 AM ICN / DCI (PCH) Feedback about proposed legislation as a stakeholder

Hello, my name is Rose Kalemba & I am a

As a stakeholder/impacted person,

I want to share my thoughts on the proposed legislation. I want to share concerns I have for multiple marginalized individuals & groups who I feel were not consulted about this proposed

legislation, including outspoken survivors like myself & many others who have been on the frontlines spreading awareness about issues with platforms, as well as sex workers & undocumented people who are often harmed & treated as collateral damage in policies that we are told will help trafficking victims, but don't truly do so in a tangible way & instead put other marginalized groups- often ones we ourselves are a part of, too, in more danger.

I am especially considered about what sounds to be getting law enforcement being involved without the victims express consent, because as an indigenous trafficking survivor I was mistreated gravely by the police when I reported my assault, & multiple family members of mine have also been victims of physical police brutality. As an advocate of over a decade, the vast majority of fellow victims I've helped do not trust law enforcement in any capacity & for good reason. Forcing marginalized people to work with law enforcement will likely lead to many victims reporting abuse of themselves online.

I know that it says in the outline that multiple marginalized & affected parties were consulted, but I don't know a single survivor or sex worker or those of us who are both who was consulted about this, & in fact our concerns have been largely ignored while self-appointed "advocates" with no lived experience speak over us.

Thank you for taking the time to read this email. I have a multitude of other concerns, but am having difficulty typing right now because of a chronic health condition but wanted to share at least some of them before the deadline.

Sincerely, Rose Kalemba





September 24, 2021

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St Gatineau QC K1A 0S5

SUBMITTED VIA EMAIL TO pch.icn-dci.pch@canada.ca

Re: The Government of Canada's proposed approach to address harmful content online

Dear Department of Canadian Heritage:

Access Now<sup>1</sup> writes to express its concerns regarding the Government of Canada's (the "Government") proposed approach to address harmful content online released on July 29, 2021.<sup>2</sup> The Government's goals are laudable as everyone, including the Government, should seek to reduce harmful speech, including hate speech, online. However, the Government's proposal will not achieve these goals. Instead, the proposed framework threatens fundamental freedoms and human rights.

The Government should ensure any legislative framework enacted into law protects human rights, including the rights to freedom of expression and speech, while also making it easier to address illegal content, hate speech, and other harmful online content. With this in mind, Access Now offers human rights-centered guidelines for content governance and urges the Government to substantially revise its approach to comply with international standards. Specifically, Access Now argues that the Government should reconsider the scope of vague definitions and overly broad categories of "harmful content," provide adequate time frames for content removal, avoid imposing proactive monitoring or filtering obligations, make fines and other sanctions proportionate, and refrain from mandating overly broad website blocking at the internet service provider level.

<sup>&</sup>lt;sup>1</sup> Access Now is an international human rights organization that defends and extends the digital rights of people at risk across the globe. This includes ensuring that individuals and groups, particularly those marginalized, do not become victims of censorship, whether through government policies or corporate practices. *See* https://www.accessnow.org/.

<sup>&</sup>lt;sup>2</sup> Have your say: The Government's proposed approach to address harmful content online, Government of Canada, (July 29, 2021) https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html.

## Reconsider the scope of vague and overly broad categories of "harmful content"

Legal clarity, precise definitions, and a narrowly tailored scope of a legislative proposal are essential preconditions to the proper functioning of the rule of law. Yet, the broad categories established in the proposal are too vague and overly broad. The technical paper incorporates five categories of harmful content: terrorist content; content that incites violence; hate speech; non-consensual sharing of intimate images; and child sexual exploitation content. It states that definitions for various categories of "harmful" content will be borrowed from the Criminal Code and "adapted to the regulatory context."<sup>3</sup> While the proposal seeks to tackle "potentially illegal content falling within the five categories of speech identified as harmful," it is also aimed at potentially harmful but *legal* categories of user-generated content, such as "material relating to child sexual exploitation activities that may not constitute a criminal offence, but when posted on an OCS is still harmful to children and victims."<sup>4</sup>

Legislation that imposes burdens on online platforms' content moderation practices should be limited to illegal content only. The principle of legality requires that offenses should be "clearly defined in the law" and "foreseeable for any person."<sup>5</sup> The proposal, however, falls short of satisfying the principle of legality because of its overly broad definitions and scope. Potentially legal but "harmful" content is an inherently vague concept that is difficult for platforms to define and the government to enforce; thus, a government mandate to police such content is highly prone to human rights abuse as companies take down more content than is necessary.

For example, the technical paper defines terrorist content as "content that actively encourages terrorism and which is likely to result in terrorism."<sup>6</sup> This is a very broad definition of (illegal) terrorist content that omits the element of intent, which should be a facet of all elements constituting terrorist criminal offences and, in fact, is an element of Canada's definition of terrorist activity.<sup>7</sup> Without considering the intention of the poster, there is a serious risk that any user-generated content related to terrosism, including news reporting, academic research, or historical resources, will be automatically deleted when flagged. Such a measure does not comply with the constitutional safeguards of a democratic society.

<sup>7</sup> Criminal Code, R.S.C. 1985, c. C-46, s. 83.01 ("terrorist activity means ... an act or omission ... (i) that is committed (a) in whole or in part for a political, religious or ideological purpose, objective or cause, and (b) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security ... and ... (ii) that intentionally" causes death, serious bodily harm, endangers someone's life, and causes serious property damage, among other things).

<sup>&</sup>lt;sup>3</sup> Technical Paper, Para. 8.

<sup>&</sup>lt;sup>4</sup> Technical Paper, Para. 8.

<sup>&</sup>lt;sup>5</sup> Daniel Gradinaru, The Principle of Legality, Proceedings of the 11th International RAIS Conference, (Nov. 19-20, 2018), http://rais.education/wp-content/uploads/2018/11/044DG.pdf; see also Practice Relating to Rule 101: The Principle of Legality, IHL Database, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2\_rul\_rule101. <sup>6</sup> Technical Paper, Para. 8.

Overly broad and opaque legal definitions will ultimately lead to an unnecessary and disproportionate interference on the right to freedom of expression. One of the dangers of overly-broad definitions for "harmful" content is that a content moderation professional with no legal training could quickly resort to bias in deciding which content to remove. This type of chilling effect has a disparate impact on marginalized communities, including communities of color, religious groups, and LGBTQ+ individuals. For example, a U.S. law intended to penalize sites that hosted speech related to child sexual abuse and trafficking led large and small internet platforms to censor broad swaths of speech with adult content.<sup>8</sup> Instead, the consequences of this censorship devastated the community the legislation sought to protect.<sup>9</sup>

Nevertheless, legislators can still address potentially "harmful" but legal content by regulating Online Communication Service Providers ("OCSPs") processes and systems for content moderation and content curation. This approach includes legally mandated criteria of meaningful transparency, due process requirements to enforce platforms' community standards, independent auditing of these systems, and other due diligence safeguards. However, the role of public regulators should be limited to public oversight, ensuring that content moderation and content curation systems are sufficiently transparent and that people have clear and compelling grievance and redress mechanisms available to them. The Government can find an example of such a novel approach in the proposed Digital Services Act of the European Union currently being debated in the European Parliament or in the PACT Act in the United States.<sup>10</sup>

Access Now urges the Government to reconsider the scope of its definitions for "harmful" content to ensure clarity in the law and avoid overly broad content takedowns.

#### Provide adequate timeframes for removing flagged content

The timeframes for removing flagged content are onerous and will lead to significant impacts on freedom of expression and speech. The technical paper proposes that OCSPs "address all content that is flagged by any person in Canada as harmful content expeditiously."<sup>11</sup> The term expeditiously is

https://www.aclu.org/sites/default/files/field\_document/aclu\_sex\_work\_decrim\_research\_brief\_new.pdf; Karen Gullo and David Greene, With FOSTA already leading to censorship, plaintiffs are seeking reinstatement of their lawsuit challenging the law's constitutionality, EFF (Mar. 1, 2019),

<sup>10</sup> Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Dec. 15, 2020),

<sup>&</sup>lt;sup>8</sup> Elliot Harmon, How Congress Censored the Internet, EFF (Mar. 21, 2018),

https://www.eff.org/deeplinks/2018/03/how-congress-censored-internet.

<sup>&</sup>lt;sup>9</sup> Is Sex Work Decriminalization the Answer? What The Research Tells Us, ACLU (Oct. 21, 2020),

https://www.eff.org/deeplinks/2019/02/fosta-already-leading-censorship-we-are-seeking-reinstatement-our-lawsuit.

https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-parliament-and-council-singlemarket-digital-services-digital-services; PACT Act, S. 797, Congress.Gov, https://www.congress.gov/bill/117thcongress/senate-bill/797.

<sup>&</sup>lt;sup>11</sup> Technical Paper, Para. 11(A).

defined as "twenty-four(24) hours from the content being flagged."<sup>12</sup> The Governor in Council has the authority to adjust this timeframe for different types of harmful content, including the power to shorten the timeline.<sup>13</sup> Within that timeline, OCSPs have two options: if flagged content qualifies as "harmful," the OCSP must remove the content from its platform; if flagged content does not qualify as "harmful" the OCSP must provide an explanation to the person who reported the content as to why it does not fall under the definition of harmful content.<sup>14</sup> OCSPs that violate the framework are subject to financial penalties of up to three percent of global revenue or \$10 million.<sup>15</sup>

A twenty-four-hour deadline to determine whether online speech meets the definition of harmful content and should be removed from a platform is an unreasonable and onerous obligation. Without adequate time to make a content moderation decision, OCSPs will by default remove flagged content regardless of its illegality or harmfulness. Content moderators are often overworked, have many cases to review, and are not truly qualified to make legal determinations. This makes over-reliance on legal criteria and inadequate, biased, or subjective censorship of content inevitable under harsh restrictive time frames for content removals. With such a short timeframe for review, it would be almost impossible for a content moderator to understand the full context of certain content. And for OCSPs that operate in multiple time zones, short time frames allocated for response would likely impose onerous burdens on smaller OCSPs with limited staff. Even worse, the harsh twenty-four hour deadline for content removals could compel OCSPs to deploy automated filtering technologies at a scale that could further result in the general monitoring of online content, ultimately violating the rights to freedom of expression and privacy.<sup>16</sup> Any revisions to the proposal should consider these nuances and the capabilities of smaller OCSPs on the market.

Strict and short deadlines for content removals cannot be reconciled with international human rights law especially when other recent proposals that follow the same proposed approach to censoring online speech are under heightened constitutional scrutiny. For example, the Constitutional Council of France declared short deadlines for removing online hate speech and other types of illegal content unconstitutional due to their negative impact on the right to freedom of expression.<sup>17</sup> According to the Council "[t]he shortness of the period left to the operators to proceed with this withdrawal, coupled with the difficulty for them to determine whether or not the comments are manifestly illegal, will encourage them to remove any content flagged as potentially illegal.<sup>218</sup>

<sup>&</sup>lt;sup>12</sup> Technical Paper, Para. 11(B).

<sup>&</sup>lt;sup>13</sup> Technical Paper, Para. 11(C).

<sup>&</sup>lt;sup>14</sup> Technical Paper, Para. 11(B).

<sup>&</sup>lt;sup>15</sup> Technical Paper, Para. 108.

<sup>&</sup>lt;sup>16</sup> See below, section entitled "Do not impose proactive monitoring or filtering obligations."

<sup>&</sup>lt;sup>17</sup> Press Release, Victory! French High Court Rules That Most of Hate Speech Bill Would Undermine Free Expression (June 18, 2020), https://www.eff.org/press/releases/victory-french-high-court-rules-most-hate-speech-bill-would-undermine-free-expression.

<sup>&</sup>lt;sup>18</sup> Decision n ° 2020-801 DC of June 18, 2020, The Constitutional Council of France, https://www.conseilconstitutionnel.fr/decision/2020/2020801DC.htm.

Another similar and controversial law, the German Network Enforcement Act ("NetzDG"), compels platforms to take down "manifestly illegal" content within 24 hours.<sup>19</sup> Several critics have pointed out NetzDG's severe implications on free speech online.<sup>20</sup> In his critique of the German law, the U.N. Special Rapporteur on Freedom of Expression reaffirmed that "[s]trict time periods of 24 hours ... coupled with ... severe penalties, could lead social networks to over-regulate expression - in particular, to delete legitimate expression, not susceptible to restriction under human rights law, as a precaution to avoid penalties.<sup>21</sup> In 2018, Human Rights Watch called the German law flawed critiquing it for being "vague, overbroad, and turn[ing] private companies into overzealous censors to avoid steep fines, leaving users with no judicial oversight or right to appeal.<sup>22</sup>

Under the international human rights framework, Canada must ensure that its policies and laws do not restrict the right to freedom of expression. Unfortunately, the Government's proposal mirrors the most harmful aspects of the worst intermediary liability regimes around the world. It presents a strong incentive for companies to remove speech to ensure compliance, even if it is not harmful or illegal. Access Now recommends that the Government replace the twenty-four content removal timeframe with a system that balances free speech, the capabilities of the OCSPs and protects Canadians against harmful content. At a minimum, the Government should revise the proposal to allow additional time to engage in a contextual analysis of flagged content. Different types of harmful online content may require different responses tailored to the specific type of content.

#### Do not impose proactive monitoring or filtering obligations

Proactive monitoring and filtering obligations from the government are particularly severe impositions. The technical paper requires OCSPs to "take all reasonable measures, which can include the use of automated systems, to identify harmful content that is communicated on its [platform] and that is accessible to persons in Canada."<sup>23</sup> Thus, the proposal imposes a general obligation to monitor content and places the burden on OCSPs to identify content for removal.<sup>24</sup> General monitoring obligations compel OCSPs to monitor content shared on their platforms indiscriminately and for an unlimited amount of time.

<sup>&</sup>lt;sup>19</sup> Overview of the NetzDG Network Enforcement Law, Center for Democracy and Technology (July 17, 2017), https://cdt.org/insights/overview-of-the-netzdg-network-enforcement-law/.

<sup>&</sup>lt;sup>20</sup> Diana Lee, Germany's NetzDG and the Threat to Online Free Speech, Yale Law School Media, Freedom & Information Access Clinic (Oct. 10, 2017), https://law.yale.edu/mfia/case-disclosed/germanys-netzdg-andthreat-online-free-speech.

<sup>&</sup>lt;sup>21</sup> UN Commission on Human Rights, *Right to freedom of opinion and expression*, June 1, 2017, OL DEU 1/2017, https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf.

<sup>&</sup>lt;sup>22</sup> Germany: Flawed Social Media Law, Human Rights Watch (Feb. 14, 2018),

https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law.

<sup>23</sup> Technical Paper, Para. 10.

<sup>24</sup> Id.

General monitoring requirements imposed by governments violate human rights including the right to freedom of expression. This concept is generally accepted globally. According to the Manila Principles, OCSPs "should never be required to monitor content proactively as part of an intermediary liability regime.<sup>25</sup> The Council of Europe recommendation also warned that governments "should not directly or indirectly impose a general obligation on platforms to monitor the content they merely give access to, or which they transmit or store, be it by automated means or not.<sup>26</sup> Likewise, the United Nations advised against censorship or monitoring of online content, noting that it infringes on the right to privacy; that "such precautionary censorship would interfere with the right to seek, receive, and impart information of all kinds on the internet,<sup>27</sup> and is likely to amount to prepublication censorship.<sup>28</sup> Further, "[n]o legal provision should ever mandate, incentivize, or give platforms any sort of indication that they should be proactively filtering content before it is uploaded.<sup>29</sup>

Consequently, the Government should remove the proactive monitoring and filtering mandate from the proposal. The Government should avoid assigning responsibility to OCSPs as adjudicators of online speech and discourse. Instead, the Government should consult with human rights advocates and experts and explore proportionate and effective alternatives that provide OCSPs with a reasonable response time to flagged speech.

#### Make sanctions for non-compliance proportionate

The sanctions in the proposal are punitive and disproportionate, and instead should be proportionate to the violation. The proposal includes a penalty of 3% or \$10 million dollars, whichever is higher.<sup>30</sup> In lieu of a penalty, a potentially-offending OCSP may enter into a compliance agreement with the Digital Safety Commissioner, and violations of that agreement can be up to 5% gross global revenues or \$25 million.<sup>31</sup>

Disproportionate sanctions inevitably lead to over-compliance, harming free expression and access to information. Article 19(3) of the Universal Declaration on Human Rights lays down the conditions that

<sup>&</sup>lt;sup>25</sup> Manila principles on intermediary liability (2015), https://www.manilaprinciples.org/.

 <sup>&</sup>lt;sup>26</sup> Council of Europe (2018), Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of Internet intermediaries, https://rm.coe.int/1680790e14 intermediaries.
 <sup>27</sup> UN Commission on Human Rights, Right to freedom of opinion and expression (June 1, 2017) OL DEU 1/2017, https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf; Decision n° 2020-801 DC of June 18, 2020, The Constitutional Council of France, https://www.conseil-

constitutionnel.fr/decision/2020/2020801DC.htm.

 <sup>&</sup>lt;sup>28</sup> UN Commission on Human Rights, *Right to freedom of opinion and expression* (April 6, 2016) A/HRC/38/35 Para
 67, https://www.undocs.org/A/HRC/38/35.

<sup>&</sup>lt;sup>29</sup> Eliska Pirkova & Javier Pallero, 26 Recommendations on Content Governance, Access Now (Mar. 3, 2016), https://www.accessnow.org/cms/assets/uploads/2020/03/Recommendations-On-Content-Governancedigital.pdf.

<sup>&</sup>lt;sup>30</sup> Technical Paper, Para 108.

<sup>&</sup>lt;sup>31</sup> Technical Paper, Para 119.

any restriction on freedom of expression must satisfy: any restrictions on speech must be lawful, necessary to achieve a legitimate aim, the least restrictive means available, and proportionate to the aim pursued.<sup>32</sup> The U.N. Special Rapporteur has already warned that "high fines raise proportionality concerns and may prompt social networks to remove content that may be lawful."<sup>33</sup> Moreover, the International Covenant on Civil and Political Rights states, "governments may only impose restrictions on freedom of expression for reasons of national security or other pressing public need if they are provided by law and are strictly necessary and proportionate for achieving a legitimate aim." Similarly, the principle of proportionality in Canadian jurisprudence requires that a measure be reasonably necessary to achieve an objective and the least intrusive method.<sup>34</sup>

As written, the proposal combines a short content takedown regime with stiff monetary penalties for non-compliance — the perfect cocktail for mass-removal of content. While the system provides harsh fines for OCSPs who leave up "harmful" content beyond twenty-four hours, there is no penalty for taking down legal speech. With those incentives, it will naturally lead to over-removal of content. Therefore, the Government's approach raises proportionality concerns and represents an undue interference with a fair assessment of whether content violates the proposal. Any new or revised regulation should ensure that sanctions imposed on OCSPs operating in Canada are proportionate to the objectives of the legislation.

#### The government should not force removal of websites without clear standards

Government-mandated website takedowns are particularly harmful without especially clear standards. The proposal grants the Digital Safety Commissioner the authority to apply to the Federal Court for an order requiring certain Telecommunications Service Providers to "block access in whole or in part to" an offending OCSP that repeatedly refuses to comply with requests to remove child sexual exploitation or terrorist content.<sup>35</sup>

As a general matter, website blocking is a blunt measure that interferes with freedom of expression and has been condemned as a violation of human rights by the United Nations.<sup>36</sup> Canada recently

<sup>35</sup> Technical Paper, Para 120.

<sup>&</sup>lt;sup>32</sup> United Nations (1966), International covenant on civil and political rights, Article 19, http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.

<sup>&</sup>lt;sup>33</sup> See UN Commission on Human Rights, Right to freedom of opinion and expression (June 1, 2017) OL DEU 1/2017, https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf; see also Decision n ° 2020-801 DC of June 18, 2020, Constitutional Council of France, https://www.conseilconstitutionnel.fr/decision/2020/2020801DC.htm.

<sup>&</sup>lt;sup>34</sup> Baker McKenzie, Proportionality in Sentencing (Canada): White Collar Offenders Beware, Lexology (Jan. 11, 2016), https://www.lexology.com/library/detail.aspx?g=67364fc2-9cda-4165-a848-52e074d6a85d.

<sup>&</sup>lt;sup>36</sup> Michael Geist, UN Special Rapporteur for Freedom of Expression: Website Blocking Plan "Raises Serious Inconsistencies" With Canada's Human Rights, Michael Geist Blog (Mar. 31, 2018),

https://www.michaelgeist.ca/2018/03/un-special-rapporteur-for-freedom-of-expression-bell-coalition-websiteblocking-plan-raises-serious-inconsistencies-with-canadas-human-rights-obligations/; see UN Commission on Human Rights, *RE: Application to Disable On-line Access to Piracy Sites, CRTC File No 8663-A182- 201800467* (Mar.

proposed a similar takedown system for "piracy" websites.<sup>37</sup> In response, the U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression warned the Canadian Government against implementing a website blocking regime, noting that blocking "raises serious inconsistencies with Canada's obligations under Article 19 of the International Covenant on Civil and Political Rights and related human rights standards," particularly the necessity and proportionality of the requirement.38

While the proposal requires a federal court to decide legality, website takedowns are limited to terrorist content and child sexual exploitation, which as described above have the broadest and most difficult definitions. An OCSP may have legitimate reasons not to remove certain content, especially that the content was not illegal and did not, in its view, violate any of the vague definitions, but may still result in full takedowns for refusing to take the content down. By combining the threat of website blocking with opaque and overly broad definitions, the Government is incentivizing OCSPs to censor any content related to terrorism or child sexual exploitation to avoid non-compliance. Even the "mere threat of blocking may have a significant and disproportionate chilling effect on its operation" as OCSPs would be inclined to take down lawful content rather than risk being shut down, as has occurred in other countries that have implemented website blocking.<sup>39</sup> The Government should therefore remove these provisions.

## Conclusion

The Government should avoid internet legislation, such as the instant proposed legislation, that endangers freedom of expression, speech, and information online. The obligations in the legislation impose unrealistic requirements on OCSPs and pose grave risks to human rights. The Government's proposal has several deficiencies and should be amended consistent with these comments, or abandoned.

<sup>29, 2018),</sup> https://services.crtc.gc.ca/pub/ListeInterventionList/Documents.aspx?ID=272698&en=2018-0046-7&dt=i.

<sup>&</sup>lt;sup>37</sup> See Michael Geist, The Case Against the Bell Coalition's Website Blocking Plan Part I: Canada's Current Copyright Law Provides Effective Anti-Piracy Tools, Michael Geist Blog (Feb. 12, 2018),

https://www.michaelgeist.ca/2018/02/case-bell-coalitions-website-blocking-plan-part-1-canadas-currentcopyright-law-provides-effective-anti-piracy-tools/.

<sup>&</sup>lt;sup>38</sup> UN Commission on Human Rights, RE: Application to Disable On-line Access to Piracy Sites, CRTC File No 8663-A182-201800467 (Mar. 29, 2018),

https://services.crtc.gc.ca/pub/ListeInterventionList/Documents.aspx?ID=272698&en=2018-0046-7&dt=i 39 Id.

#### Submissions on Government of Canada's Technical Paper re: Proposed Approach to Online Harms

#### Submitted by Prof Jane Bailey<sup>\*</sup> and Dr Valerie Steeves<sup>\*\*</sup> Co-Leaders of <u>The eQuality Project</u> University of Ottawa

We have prepared this submission in response to the call for comments on the <u>Government of</u> <u>Canada's Technical Paper</u> relating to its proposed approach to online harms, dated 29 July 2021. The submission is grounded first and foremost on key principles from the <u>UN Convention on the</u> <u>Rights of the Child</u> (CRC). It is also based on the authors' decades of involvement in researching and advocating for the rights of young people, especially in a digitally networked world, including Canadian research findings from: The eQuality Project,<sup>i</sup> The eGirls Project<sup>ii</sup> and MediaSmarts' Young Canadians in a Wired World Project (YCWW).<sup>iii</sup>

## GENERAL COMMENTS

As a signatory to the CRC, Canada is obligated to ensure that its laws *provide* children with access to their rights, *protect* children from harm (including protection from discrimination (Art. 2(2)), and enable children to *participate* in decisions that affect them. Networked media play an important role in meeting these obligations as the CRC guarantees children:

- the right to free expression, including the right to access information and ideas from a range of national and international sources through a child's preferred choice of media (Arts. 13 and 17)
- the right to free association (Art. 15)
- the right to education (Art. 28), especially education that supports the child's personal and cultural identity and values (Art. 29)
- the right to play (Art. 31)
- the right to participate in cultural and artistic life (Art. 31)
- the right to privacy (Art. 16)<sup>iv</sup>

Networked media are therefore useful tools for advancing child rights because they provide access to a wealth of cultural, educational and artistic information, and create new avenues for community-building, education, play and artistic expression.

Simultaneously, however, networked media also facilitate distribution of hateful content, nonconsensual distribution of intimate images, child sexual abuse imagery and other forms of harmful content that circumscribe children's ability to fully benefit from access to networked media, as well as their rights to full societal participation in a seamlessly integrated online/offline world. The rights of children from communities marginalized by racism, sexism, homophobia, transphobia, colonialism, ableism and other systemic oppressions and their intersections are particularly likely to be negatively affected by harmful online content, directly undermining their right to *protection* from discrimination.

<sup>\*</sup> Full Professor, University of Ottawa Faculty of Law (Common Law), co-leader of <u>The eQuality Project</u>, previously co-leader of <u>The eQuality Project</u>.

<sup>\*\*</sup> Full Professor, University of Ottawa Department of Criminology, co-leader of The eGirls Project and The eQuality Project, previously Lead Researcher for MediaSmarts' Young Canadians in a Wired World research project.

Further, the commercial model driving networked platforms has constrained the potential of networked media to advance children's rights, precisely because online communication service providers (OCSP) seek to collect as much information as possible from users so their behaviours and attitudes can be commodified. As Shosana Zuboff notes:

... young life now unfolds in the spaces of private capital, owned and operated by surveillance capitalists, mediated by their 'economic orientation,' and operationalized in practices designed to maximize surveillance revenues. These private spaces are the media through which every form of social influence—social pressure, social comparison, modeling, subliminal priming—is summoned to tune, herd, and manipulate behavior in the name of surveillance revenues" (Zuboff, 2019, p. 456).

The information that is collected is then processed by algorithms that categorize children for commercial purposes, with two problematic results. First, algorithms tend to privilege extreme representations because they attract more views and therefore generate more revenue (Berger & Milkman, 2012). This degrades the networked public sphere, making it more difficult for children, especially those belonging to marginalized communities, to participate in social and political discourse. Second, algorithms tend to (re)produce discrimination grounded in racism, sexism, homophobia, transphobia, colonialism, ableism and other systemic oppressions and their intersections, and to do so in non-transparent and therefore non-accountable ways (Burkell & Bailey, 2016-2018).

The lack of privacy at the heart of the commercial model and its related discriminatory impacts are further exacerbated by the fact that policymakers – who are seeking to protect children – have typically relied upon surveillance and punishment to curb individual bad actors. The over-privileging of this particular approach to *protection* has often made it more difficult for children to *participate* in networked spaces (Steeves, 2012). Again, this is particularly harmful for young Canadians from marginalized communities that are already under-served and over-policed. For example, networked media can be an important source of both information and community for LGBTQ youth (Craig and McInroy, 2014) and our most recent data (unpublished) suggest that commercial and protective surveillance are making it increasingly difficult for LGBTQ youth to explore their sexuality online precisely because they know they are being watched.

In order to balance their rights to *provision*, *protection* and *participation*, our young research participants call for correctives that will reduce the structural harassment that too often defines their online interactions (Bailey & Steeves, 2015; Bailey & Steeves, 2017; Brisson-Boivin, 2019). This would require the enforcement of existing laws that deal with illegal content (e.g. criminal prosecutions against those who utter threats or advocate genocide, or post intimate images without consent), new regulations that will hold platform companies to account for the ways that they contribute to online harms, as well as policy initiatives to support them in dealing with online harms (Bailey & Burkell, 2020) (including by funding community organizations that serve youth), and to proactively address the systemically discriminatory root causes of many forms of online harm, through research, educational and other similar initiatives (Bailey, 2015).

#### SPECIFIC PROVISIONS

Paragraph 2

• The definition of private communication should be consistent with young people's understanding of privacy as the inter-subjective negotiation of the boundary between self and other (Steeves, 2015). From this perspective, young people's privacy rights do not

disappear just because they have posted information on an app or service that an OCSP defines as "public".

#### Paragraph 8

- The five types of content are very different and each category requires a specialized approach, which may well merit entirely separate regulatory regimes for each one. For example, while a 24-hour takedown rule could be very important and effective in the context of clear cases of the non-consensual sharing of intimate images, it would provide very little time for meaningfully addressing the nuances of what could be captured by "terrorist content". It is particularly important to take a nuanced approach to these different types of content, given the potential for a direct line to law enforcement and/or CSIS (under Paragraph 20). Sharing information without the consent of the individuals directly affected by certain kinds of content may further erode what is often an already-eroded sense of agency; it is likely also to play into pre-existing discriminatory stereotypes that disproportionately expose members of many marginalized communities to greater surveillance and punishment.
- Translating *Criminal Code* definitions of harm, that often seek to balance rights by distinguishing between public and private communications, may be difficult. Drafters should take young people's understanding of online privacy into account to ensure that regulations do not shut down important avenues for young people to communicate. This is especially true of members of marginalized groups who are already over-policed and, frequently more at risk of being censored.
- Drafters should conduct a child rights assessment review to ensure that all types of content that are included in any future legislation take children's special interests into account. For example, child sexual exploitation provisions should expressly exclude sexual information in the best interests of a child (especially for members of marginalized communities such as LGBTQ youth).

#### Paragraph 10

- Algorithms may or may not be able to identify harmful content, depending on the category of harm. Again, a one-size-fits-all approach is unlikely to address the nuances of each type of content.
- Given the evidence that algorithms (re)produce discrimination, it is crucial that strong
  measures be enacted to ensure that automated decision-making processes are both
  transparent and accountable.

## Paragraph 12

 Internal safeguards and/or ex post facto oversight will not protect the best interests of the child because neither can counterbalance the demands of the OCSP business models to monetize and nudge young people. We need proactive public administrative bodies that young people can access for both intervention and support in relation to harmful content posted on OCSPs. Young people should be able to access that support without having to first "exhaust" all other private avenues (as per paragraph 50).

Paragraph 14

Requiring OCSPs to issue reports is a necessary first step towards transparency and
accountability. It will be important to require OCSPs to itemize how they monetize
harmful content, and to avoid reframing the business model as protective merely because
it facilitates surveillance. It will also be important to require OCSPs to produce data that
sheds light on the social locations of the communities that are targeted, any intersecting
axes of discrimination involved, who the perpetrators/sources are (where possible), and
the content of the material that has been evaluated to facilitate the identification of any
discriminatory trends in content and in OCSP approaches to content.

#### Paragraphs 20-33

- Considering the disproportionate impacts the proposals in these paragraphs could have on members of Black, Indigenous and other over-policed and over-surveilled marginalized communities who have strong historic reasons for not wanting to involve law enforcement agencies in their lives, reforms should be focused on providing support for those targeted by harmful content instead of the creation of a direct pipeline from the OCSP to law enforcement.
- At the very least, the informed consent of adults targeted by content such as nonconsensual distribution of intimate images should be required to be obtained prior to disclosure to law enforcement. This will be especially important for targeted individuals whose agency has already been undermined by online content, and/or who are members of communities with strong historic reasons not to trust law enforcement agencies.

#### Paragraph 35

The Digital Safety Commissioner should have a stronger mandate to directly support
affected community members and proactive powers to call platforms to account (i.e. not
just complaints based and after the fact).

#### Paragraph 48

• The small size of the Digital Recourse Council will make it difficult to ensure the Council has appropriate community input. Especially since the lived experience of the harm will vary according to the context of the content, provisions should be added to insure meaningful representation of affected communities.

## Paragraph 50

• Persons should be able to initiate a complaint with the Digital Recourse Council without first exhausting the internal OSCP complaints process. Young people repeatedly report that OSCP processes are ineffective and slow, so being forced to wait until after jumping through so many hoops in order to obtain a remedy will be meaningless to most.

## Paragraph 59

• Balancing young people's rights to *provision*, *protection* and *participation* requires an open and active public debate and full transparency with respect to commercial practices (especially those that involve algorithms). Hearings should accordingly only be held *in* 

*camera* in the most unusual of circumstances. In particular, protecting confidential commercial interests should never by itself be enough to justify an *in camera* hearing.

#### Paragraph 83

While the Digital Safety Commissioner and the Digital Recourse Council should have the
power to redact the names of complainants and posters, this power should never extend to
commercially sensitive information. Redacting commercial information would restrict
the transparency that is required to hold OSCPs accountable.

#### GENERAL RECOMMENDATIONS

- The government should not proceed to enact any provisions recommended in the Technical Paper without first conducting open, widespread, and intersectionally-diverse consultation. In particular, young people need to be directly engaged in the policy development process, in keeping with their CRC right to *participate* in decisions that affect them.
- Any reforms should take into account the fact that public bodies, such as administrative agencies, are better able than corporations to balance public/private and rights/harms. They are more accountable due to their public nature, and their actions will be directly constrained by the *Charter*.
- Once a draft Bill is available, the government should conduct a child rights impact
  assessment to ensure that reforms respect all of the media and anti-discrimination rights
  set out in the CRC.

All of which is respectfully submitted:

Jane Bailey Co-Leader of The eQuality Project

Valerie Steeves Co-Leader of The eQuality Project

## WORKS CITED

Bailey, J. and Steeves, V. (2015). eGirls, eCitizens. Ottawa: University of Ottawa Press.

Bailey, J. (2015). A perfect storm: How the online environment, social norms and law constrain girls' online lives. In J. Bailey and V. Steeves (Eds.), *eGirls, eCitizens*, Ottawa: uOttawa Press.

Bailey, J. and Steeves, V. (2017). Defamation law in the age of the internet: Young people's perspectives. Commissioned by the Law Commission of Ontario. Online: http://www.lcocdo.org/wp-content/uploads/2017/07/DIA-Commissioned-Paper-eQuality.pdf. Retrieved 23 September 2021.

Bailey, J. and Burkell, J. (2020). Legal remedies for online attacks: Young people's perspectives. *The Annual Review of Interdisciplinary Justice Research*, 9, 110.

Burkell, J. and Jane Bailey. (2016-2018). Unlawful distinctions?: Canadian human rights law and algorithmic bias. *Canadian Yearbook of Human Rights*, 217.

Steeves, V. (2015). Privacy, sociality and the failure of regulation: Lessons learned from young canadians' online experiences. In Beate Roessler and Dorota Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives*. Cambridge, UK: Cambridge University Press, pp. 244-260.

Steeves, V. (2012). Young Canadians in a wired world, phase III: Talking to youth and parents about life online. Ottawa: MediaSmarts.

Steeves, V., McAleese, S. and Brisson-Boivin, K. (2020). Young Canadians in a wireless world, phase IV: Talking to youth and parents about online resiliency. Ottawa: MediaSmarts.

<sup>&</sup>lt;sup>1</sup> <u>The eQuality Project</u> is a 7-year SSHRC funded partnership focused on better understanding young people's experiences with privacy and equality in digitally networked environments. This submission draws in particular from findings in our <u>2017 report</u> prepared for the Law Commission of Ontario entitled *Defamation Law in the Age of the Internet: Young People's Perspectives.* That report was based on interviews that eQuality Project researchers conducted with 20 young people aged 15-21 in Ontario in February and March of 2017. The purpose of the interviews was to explore young people's attitudes toward and experiences with online defamation, reputation, anonymity, and the benefits and drawbacks of existing mechanisms for addressing online defamation. The interview discussion guide, consent documents, recruitment text and method of analysis were approved by the University of Ottawa Research Ethics Board.

<sup>&</sup>quot;The eGirls Project was a 3-year SSHRC funded partnership development initiative focused on better understanding the experiences of girls and young women in digitally networked environments. In January and February of 2013 researchers with The eGirls Project held a series of interviews and focus groups with girls and young women between the ages of 15 and 22. All participants used interactive online media (such as social networking, blogging and/or user generated video sites) as a regular part of their social lives. Half of our sample resided in an urban Ontario setting and half resided in a rural Ontario setting. We interviewed six girls aged 15-17 and six young women aged 18-22, for 60-90 minutes each. An additional 22 participated in four focus group discussions, as follows: (1) seven girls aged 15-17 living in the urban setting; (2) five girls aged 15-17 living in the rural setting; (3) six young women aged 18-22 living in the urban setting and (4) four young women aged 18-22 living in the rural setting. Focus group discussions were approximately 90 minutes in length. A professional research house recruited our participants on the basis of sex, age (either 15-17 or 18-22) and location of residence (urban or rural). While participants were not recruited on the basis of self-identification with regard to other aspects of their identities, such as race, ethnicity, gender identity or sexual orientation, our participant group included members of racialized, linguistic, and various religious groups. In the interviews and the focus groups, we explored, among other things, the types of visual and textual representations the participants used online to express their identity as young women, and the benefits and pitfalls they experience on social media. We also asked for their views on the issues and policy responses focused upon by policymakers and explored their understandings of networked privacy and equality. With participant permission, the interviews and focus groups were audiotaped and transcribed by our research assistants for analysis. The transcripts were then subjected to a thematic qualitative analysis. All identifying information was removed from the transcripts, and pseudonyms are used below to identify participants: for a full report see eGirls eCitizens, Jane Bailey and Valerie Steeves (eds) online: https://press.uottawa.ca/open-access/egirls-ecitizens.html. iii MediaSmart's Young Canadians in a Wired World project began in 2000-2001 with interviews of parents and children, and a survey of approximately 5,500 Canadian students aged 10 to 17, to examine children's use and perceptions of the Internet. In 2004-2005, Steeves become the lead researcher for the project, and conducted a similar study, broadening the technology to other forms of networked communications, including cell phones and

gaming platforms. In 2012-2013, Steeves again returned to the field, conducting 12 qualitative focus group sessions (four each in Calgary, Toronto and Ottawa) with a total of 66 young people aged 11-17 and 21 parents of children and youth aged 11-17 and a quantitative survey of 5,436 children and youth aged 10-17 from across the country, as well as conducting interviews with 10 key informant teachers from across the country to get a better understanding of the impact of the full range of networked technologies in the classroom. In 2020, Steeves worked with Brisson-Boivin and McAleese and conducted three focus group sessions, in Ottawa, Toronto and Halifax respectively, with 34 young people aged 11 to 17 and 8 parents with children aged 11 to 17 to explore what is and what is not working for young people in networked spaces. For a full report of each phase of YCWW, see http://mediasmarts.ca/research-policy.

<sup>iv</sup> See Steeves, Valerie. (2018). Snoops, Bullies and Hucksters: What Rights Do Young People Have in a Networked Environment? In Nancy A. Jennings and Sharon R. Mazzarella (eds.), 20 Questions about Youth and the *Media*. New York: Peter Lang.

(Jacosmini communique en initia pri la Jat sur l'acolo d'influencian (Document Reen iso que unit) l' the Access to Programment Inc.



# Living in Community

# Submission regarding the federal government's proposed approach to address harmful content online

From Living in Community Society

Submitted by Halena Seiferling, Executive Director director@livingincommunity.ca September 22, 2021



# Living in Community

#### Background

Living in Community (LIC) is a provincial non-profit organization based in Vancouver, British Columbia. Centering sex workers' rights, Living in Community convenes diverse stakeholders in order to: understand a range of experiences and perspectives; inform sex work-related policies and practices of governments, service providers, and community organizations; and provide education to support these goals. We focus on root causes of issues including colonization, capitalism, criminalization, racism, and discrimination that create systemic vulnerability for sex workers, and we seek to build understanding and common ground with other community members.

As an organization that works with diverse sex workers and sex worker-serving organizations across BC, we are concerned about several aspects of the government's proposal outlined in this consultation. If implemented, this legislation would infringe upon sex workers' rights and freedoms, creating additional barriers and hardships for an already-marginalized group of workers.

Under Bill C-36, the *Protection of Communities and Exploited Persons Act*, providing a sexual service and advertising on behalf of yourself to provide sexual services are decriminalized in Canada.<sup>1</sup> While we believe this legislation is problematic and leaves the sector still criminalized and stigmatized overall, it provides an important legal basis that sex workers have the right to work.

Though the government's proposed approach may be well-intentioned to address harmful content and behavior online, this legislation would have dangerous consequences for human rights. The proposed framework and regulations are far-reaching, extremely broad, and could sweep up lawful speech and content in ways that can be misused for censorship and surveillance.<sup>2</sup>

In particular, there are several concerning aspects of this proposal which we describe in more detail below:

- 1. Proactive monitoring of content
- 2. 24-hour takedown provision
- 3. Substantial financial penalties
- 4. Mandatory reporting to law enforcement
- 5. Sweeping regulatory powers
- 6. Pushing sex work into less safe environments
- 7. Increased urgency of these issues due to COVID-19
- 8. Concerning timeline of this consultation

#### Concerns with this proposal

#### 1. Proactive monitoring of content

This proposal would require "regulated entities to do whatever is reasonable and within their power to monitor for the regulated categories of harmful content on their services, including through the use of automated systems based on algorithms."<sup>3</sup> Automated filters cannot tell the difference between content that is accurately illegal and that same content being re-used for news reporting, educating,

<sup>&</sup>lt;sup>1</sup> Government of Canada, 2014. Bill C-36, Protection of Communities and Exploited Persons Act. https://parl.ca/DocumentViewer/en/41-2/bill/C-36/royal-assent

<sup>&</sup>lt;sup>2</sup> Canadian Alliance for Sex Work Law Reform.

<sup>&</sup>lt;sup>3</sup> Government of Canada, 2021. Discussion Guide, "Have your say: The Government's proposed approach to address harmful content online." <u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html</u>



or counter-speech.<sup>4</sup> Automated filters also cannot tell the difference between an online clip of consenting adults performing their work or those forced into exploitative situations, and cannot reliably flag someone's age. This means that legal speech and content relating to sex work may be swept up in an automated filter.

Living in Community

#### 2. 24-hour takedown provision

In the framework, "regulated entities would be required to respond to the flagged content...within 24 hours of being flagged."<sup>5</sup> Such a timeline has been shown to incentivize platforms to err on the side of taking down lawful content to avoid risk and liability, as well as to include in their Terms of Service broad prohibitions on content that is legal.<sup>6</sup> In addition to infringing upon the right to share legal content, this timeframe would be extremely onerous on smaller companies or individual content creators.

#### 3. Substantial financial penalties

The framework proposes that, in some cases, penalties may be up to \$10 million or 3% of an entity's gross global revenue, whichever is higher.<sup>7</sup> As with the 24-hour takedown provision, such an overbearing financial risk would incentivize platforms and creators to avoid sharing legal content.

#### 4. Mandatory reporting to law enforcement

The proposed framework considers including basic subscriber information (BSI), which includes a customer's name, address, phone number, and billing information associated with the IP address, in the information that could be reported to law enforcement without first requiring judicial authorization.<sup>8</sup> Sweeping reporting requirements like this lead to a high likelihood of 'false positives' whereby platforms and creators sharing legal content could be reported. Sex workers are already surveilled, harassed, and discriminated against by law enforcement, even though selling sex is legal under Canadian law, and should not be made even more vulnerable to law enforcement intervention in their legal work by giving law enforcement more information with no crime being committed.

#### 5. Sweeping regulatory powers

The proposal introduces a number of new regulatory bodies as well as a Commissioner who, among other powers, would be able to "proactively inspect for compliance" and "require an OCSP [Online Communication Service Provider] to do any act or thing, or refrain from doing anything necessary to ensure compliance with any obligations imposed on the OCSP by or under the Act within the time specified in the order."<sup>9</sup> These vague and sweeping powers are cause for concern when coupled with the lack of judicial review needed in each case when we consider Canadians' rights and freedoms guaranteed under the Charter.

Moreover, under this proposal the Commissioner would also have the ability to "apply to the Federal Court to seek an order to require Telecommunications Service Providers to implement a blocking or filtering mechanism to prevent access to all or part of a service in Canada."<sup>10</sup> This type of sweeping

<sup>&</sup>lt;sup>4</sup> Keller, D., 2021. "Five Big Problems with Canada's Proposed Regulatory Framework for 'Harmful Online Content."" <u>https://techpolicy.press/five-big-problems-with-canadas-proposed-regulatory-framework-for-harmful-online-content/</u> <sup>5</sup> Government of Canada, 2021, Discussion Guide.

<sup>6</sup> Kaller D. 2021

<sup>&</sup>lt;sup>6</sup> Keller, D., 2021.

<sup>&</sup>lt;sup>7</sup> Government of Canada, 2021. Discussion Guide.

<sup>8</sup> Ibid

<sup>&</sup>lt;sup>9</sup> Ibid; Government of Canada, 2021. Technical Paper, "'Have your say: The Government's proposed approach to address harmful content online." <u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html</u>.

<sup>10</sup> Government of Canada, 2021. Discussion Guide.



ISP blocking has been criticized by international human rights experts for its infringement on the right to freedom of expression.<sup>11</sup>

jving in Community

#### 6. Pushing sex work into less safe environments

Since the sex work sector is not fully decriminalized in Canada, what we have heard and experienced from among sex workers in our communities is that the sector remains unsafe. Sex workers are routinely surveilled and harassed by law enforcement who target clients of sex workers for communicating and purchasing sex, and street-based sex workers are forced to work in more clandestine and isolated areas in order to evade law enforcement. Sex workers are often rushed in deciding whether or not to take on a client because they cannot speak openly about what services are being offered, they must make decisions quickly to avoid detection, and it is difficult to find safe indoor spaces to work as these businesses are criminalized. While limitations remain, online platforms often offer sex workers more safety as they can screen clients and have a greater degree of control over their work environment and options.

We are concerned that this legislation would push sex work into less safe environments by limiting the internet as a safer avenue. With the high risk of 'false positives' being reported as well as the onerous financial penalties, sex workers may be pushed (back) into less safe forms of sex work, like street-based work.

#### 7. Increased urgency of these issues due to COVID-19

COVID-19 has heightened the issues raised above. Many sex workers have experienced a significant or complete loss of income, have struggled to access community services because many frontline organizations have had to reduce their services and hours, and have been ineligible for government supports such as the CERB or EI. Additionally, many sex workers have pivoted to online work during COVID-19 to respect public health requirements and best practices against in-person contact.

By reducing the ability of sex workers to work online – one of the only safer options available for some sex workers – this bill would further entrench critical and systemic gaps in safety for sex workers.

#### 8. Concerning timeline of this consultation

Finally, we draw your attention to the concerning timeline of this consultation. Launched in the summer – when many folks are enjoying a much-needed break, especially after a year and a half of pandemic lockdowns – and continuing through a federal election is an inadvisable time period to hold a public consultation. If implemented, this legislation would significantly impact not only sex workers but also internet users and creators of all kinds who may not be able to fully participate in this consultation at this time.

#### Conclusion

If implemented, we are concerned that this legislation would infringe upon sex workers' legal work, would have broad and overreaching implications for surveillance and human rights, and would lead to increased safety concerns for sex workers. We ask you to carefully review these considerations and revise this proposal.

<sup>&</sup>lt;sup>11</sup> UN Special Rapporteur for Freedom of Opinion and Expression and the IACHR-OAS Special Rapporteur, Joint Declaration on Freedom of Expression. <u>https://perma.cc/8RVR-HQTJ</u>.

Secondaria - constantina e a conta por e Esta con Para - Secondaria a conta toma Marina e a conta conta e a conta por se Marina e a conta e a conta por se Marina e a conta e a conta e a conta Marina e a conta e a conta e a conta e Marina e a conta e a conta e a conta e Marina e a conta e a conta e a conta e conta e a conta e a conta e a conta e conta e a conta e a conta e a conta e conta e a conta e a conta e a conta e conta e a conta e a conta e a conta e conta e a conta e a conta e a conta e conta e a conta e a conta e a conta e conta e a conta e a conta e a conta e conta e a conta e a conta e a conta e conta e a conta e a conta e a conta e a conta e conta e a conta e conta e a conta e conta e a conta e c

To: Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St Gatineau QC K1A 0S5 pch.icn-dci.pch@canada.ca

#### From:

Maggie MacDonald, MA, PhD (S) & Valerie Webber, MA, MPH, PhD (C)

To the organizers, concerning the proposed Digital Citizen Initiative;

We appreciate the opportunity to share our expertise on the matter to inform the Government's proposal to establish a Digital Safety Commission. We are two researchers working at the intersections of sex worker regulations and digital governance. Maggie MacDonald is a SSHRC-funded doctoral researcher and PhD student at the University of Toronto's Faculty of Information with a specialization in Sexual Diversity Studies. Ms. MacDonald has published research on sex worker governance, deepfake porn, and on the digital methods used to study online platforms. Ms. Webber is a PhD Candidate in Community Health & Humanities at Memorial University of Newfoundland, studying occupational health and safety in the pornography industries. She holds degrees in Sexuality & Gender Studies, Public Health, and Medical Anthropology and has published in the areas of public health, pornography studies, and ethics. She also has over 15 years of experience as an online sex worker.

We share the government's concern regarding harmful online content and abuses. However, we believe that the proposed framework will not effectively address many of the named harms but will, in fact, exacerbate harm and increase violence against overlapping groups of people, including sex workers and labour organizers advocating for them, as well as content creators and social media users at large.

As we have discussed in <u>our recently published article</u> concerning Bill C-302, Part V of the Canadian criminal code already has strict laws governing the production and sharing of intimate images, and some of the broadest child sexual abuse material legislation in the world. In particular, Sections 162 and 163 already provide legal recourse for those who are recorded (filmed or photographed) as a minor, are recorded without their explicit consent, or have their images distributed without their explicit consent. The introduction of a proactively regulatory approach risks harming the very same equity-deserving groups that this new framework seeks to help.

Some specific proposals of concern include proactive monitoring of content, the tight turnaround time for removal of suspect content paired with steep financial penalties, the obligation to contact law enforcement before it is clear a criminal act has taken place, the access to and retention of user information, and the possibility of blocking entire platforms.

When detection and removal requirements are unrealistic, this encourages a chilling effect among platforms and providers to simply blanket-prohibit a wide range of content, rather than tighten their own moderation standards around what is being posted. Both human and automated systems for <u>flagging content as unsafe</u> disproportionately impact <u>sex workers</u>, activists and organizers, sexual health educators, <u>2SLGBTQ+people and</u> the queer community at large, as well as other purportedly protected classes and communities who are <u>routinely technologically marginalized on the basis of race</u>. <u>sexuality, and gender presentation</u>.

Given that content moderation has been proven to disproportionately target marginalized populations--indeed, the same populations this framework claims to protect--the requirement that regulated entities contact law enforcement over perceived infractions is extremely concerning for freedom of expression being stratified based on identity signifiers. Whatever the threshold for triggering such a reporting obligation, history has shown that faced with similar legislation, regulated entities will err on the side of caution around sexual material of all stripes and proactively moderate their platforms in order to avoid steep penalties. This will result in the disproportionate criminal pursuit of already targeted and marginalized people, without requiring any actual criminal offence to take place. Regulation of user content already targets non-normative sexualities and acts disproportionately and has the potential for devastating consequences on the lives of Canadians who do not conform to whiteness, able-bodiedness, or normative gender presentation, such that POC, queer, disabled, and especially sex-working Canadians will face the greatest burden of scrutiny under the new measures. That the regulated entities would be required to retain data related to these potential cases could further produce innumerable privacy and confidentiality concerns for these populations. Finally, that the regulated entities could be required to block entire online communication platforms in Canada--platforms that many sex workers use to earn a safe living--raises a tumult of free speech and human rights concerns.

This is particularly concerning given that, while the majority of child sexual abuse materials (CSAM) are not found on pornography sites but on <u>social media platforms like</u> <u>Facebook</u>, pornsites are <u>unfairly targeted</u> as <u>scapegoats to an immeasurably difficult</u>

social problem. Basing digital governance practices on unfounded claims or around media swells of moral panic will result in toothless policy as well as discriminatory frameworks. Primarily, such policy gravely harms those trying to earn a living by producing legal content for sale. When online avenues for sex work are so heavily regulated as to be rendered criminal by default, this pushes workers into other forms of sex work that are <u>explicitly criminalized</u> and <u>therefore significantly more dangerous</u>. The scapegoating of pornography provides a convenient target for public ire while neglecting <u>social media platforms</u> that circulate violence, misinformation and discriminatory content, and have been proven to house vastly greater quantities of CSAM than <u>dedicated pornography sites</u>.

We share the Government's concerns regarding the rise of white supremacist, fascist hate groups. However, we are concerned that the expansion of CSIS powers to monitor "Online Ideologically-Motivated Violent Extremist communities" will also result in context collapse that conflates those dangerous activities with sex workers, who are too frequently painted as ungovernable or amoral by antiporn and religious groups. If this framing holds without clear distinctions, it will be used to target any number of groups or associations around the 2SLGBTQ+ community and sexual subcultures, as well as workers and activist efforts around sex work who are exercising their democratic right to criticize government policy and practice.

There is a distressing trend among governments to consult primarily with groups that seek to conflate all manner of sex work with abuse and "human trafficking", and go on to develop prohibitive and ill-informed regulatory measures in response. These testimonies are not based on reliable research findings, or even meaningful consultation with industry players, and have led to mistrials in recent platform regulation. Canada has the benefit of getting to witness how similar legislative attempts to regulate online communication service providers have failed in the United States. We do not need to make the same mistakes, but have the opportunity to lead regulatory movements with evidence and consultation-based strategy. The United States Government Accountability Office recently published a report documenting the complete failure of FOSTA, the Fight Online Sex Trafficking Act of 2017. FOSTA was ostensibly intended to protect people from sexual exploitation by holding platform operators responsible for user-generated content facilitating sex trafficking. As a response, platforms instead adopted widespread censorship of all forms of sexual content, including advertising and other resources sex workers used to ensure their own safety while working. Even more potently, FOSTA has only been used a single time since its passage, and furthermore the loss of cooperative online platforms and the migration of abusers to platforms hosted overseas has made it even more difficult for the government to pursue cases of sexual exploitation and human trafficking. The conflation of sex work and abuse fails to

respect and protect the consensual choice of many individuals to earn a living through sex work, while also failing to address the actual sources of violence.

Luckily, there are a lot of sex workers and advocates, content creators, and digital rights activists who have thought long and hard about content moderation. Online sex workers in particular have long experienced having their content distributed without their consent, and having their completely consensual content unnecessarily flagged as otherwise, to be scrutinized and removed. Having knowledge of this dynamic of the system provides sex workers with a thorough and nuanced understanding of the strengths and limitations of various content moderation methods including consent paperwork and recordkeeping, identify verification, user-flagging and reporting, digital fingerprinting, DCMA takedowns, and so on. There is a wealth of sex worker knowledge available to adapt and structure these methods to the greatest benefit for all internet users, while avoiding potentially disastrous outcomes named above as well as privacy violations, stalking, and income loss, to name only a few.

When the 2013 Supreme Court decision, *Canada (AG) v. Bedford*, overturned the sections of Canada's criminal code related to prostitution, new regulatory measures (Protection of Communities and Exploited Persons Act) were introduced the following year, without sex worker consultation or consideration. These measures are egregiously hostile to sex workers and have made the landscape <u>even more dangerous to navigate</u>. Legislation and policy drafted in this same spirit will remain volatile and lack rigour. We must not commit the same offence here. Sex workers and content creators must be centered in any decision-making process regarding online content moderation in order to avoid implementing yet another set of laws intended to help, but which put lives and livelihoods at stake once enacted.

We thank you for your time and consideration. Sincerely,

Maggie MacDonald Valerie Webber

Contractor Contractory Internet (1) (1) (1) Classic Processing Contractory (1) Classic Processing Contractory (1) Contractory Contracto



# **Internet Society Canada Chapter**

# Submission to the Department of Canadian Heritage: Consultation on Internet Harms

## Who We Are

 The Internet Society Canada Chapter (ISCC) is a not-for-profit corporation that engages on internet legal and policy issues to advocate for an open, accessible and affordable internet for Canadians. An open internet means one in which ideas and expression can be communicated and received except where limits have been imposed by law. An accessible internet is one where all persons and all interests can freely access websites that span all legal forms of expression. An affordable internet is one by which all Canadians can access internet services at a reasonable price.

## Structure of this Submission

2. In this submission we will first give an overview of what ISCC believes to be the most salient points of the legal and administrative framework of the Government's Proposal with respect to the regulation of online harms ("the Proposal"). The submission will then outline what it sees as being the key critiques to be made of the Proposal. Finally, ISCC will include its comments on individual components of the Proposal that it believes merit careful consideration.

# **The Consultative Process**

- ISCC would like to register its profound disappointment with this ostensible consultative process.
- 4. First, it is taking place during an electoral period, despite the fact that its subject matter is composes parts of partisan platforms. This suggests it is inappropriate to be consulting when at least one of the parties, if successful in forming a government, has pre-empted genuine consideration of meaningful suggestions for change.

#### Internet Harms

Test of the Period a transmission interview of a the most consequent to

- 5. ISCC notes that the Guide and Technical Paper offer no alternatives and ask no questions of those wishing to make comments. Indeed, the Technical Paper has the air of drafting instructions. It leads to the conclusion that the purpose of the consultation is not to seek public input but to merely satisfy multiple target opinion groups that the Government is doing something to combat what it considers to be Internet Harms.
- 6. Neither the Technical paper nor the guide cite any studies or reports that identify the proposed harms as being the ones most urgent of legislative action, nor is it clear how the current content moderation regimes of the social media are failing, or how the Proposal would correct them in a meaningful way. While harm is assumed (and ISCC does not question that there is some harm), there appears to be no examination of alternatives to negate those harms and no research is referenced that would demonstrate that the Proposal would rectify any deficiencies in the existing content moderation regimes.
- 7. The Technical paper fails to lay out the definitions of the five listed Internet harms, but then promises both that whatever goes into the legislation will be broader than mere criminal law definitions, and then goes on to promise that whatever definitions eventually included in the legislation can be expanded upon by unilateral action of Cabinet. In other words, the central issues on which the Government proposes to legislate are not even available for consultation. As a brilliant Wendy's advertising campaign once said: "Where's the beef?". What are we really dealing with? What speech is to be subject to the censor's pen? Who is to be silenced? Who is to be protected and at what cost?
- 8. ISCC is responding to this consultation as if this is meant to be a true consultation. It does so because the harms created by the Proposal would outweigh any good arising from it. The harms of any legislation adopted based on the Proposal will negatively impact Canada and Canadians and also ripple through and poison the global Internet.

## **Introductory Overview**

- 9. Social media platforms (Facebook, Twitter, TikTok, YouTube, Parler, etc.) provide an electronic space where users can post about matters that are important to their self-expression. Much of the content that is posted relates to personal life a means to record and tell friends and acquaintances about the flow of individual and family life: the decorated tables marking the feast days, the children's birthdays, anniversaries, vacations, the chronology of a life being lived. Dear and cute grandchild and pet pictures and videos abound.
- 10. Social media platforms have also become an important element in cultural and commercial expression. Artists now both create works on social media platforms and reach audiences that could never have been accessed in earlier times. Businesses use social media to make their products and services known to a potentially global audience. Promotional how-to videos have enriched the lives of do-it-yourselfers of every stripe. Businesses also use social media intermediaries ("influencers") to promote their products and services to audiences that are resistant or unreachable by standard advertising techniques.

- 11. Social media are not merely platforms for the sharing of the incidents of personal life, cultural expression or commercial interests. They are also a means of engagement on social and political issues. They are a means of social and political organization and expression on a host of issues of contemporary importance and controversy. Social justice warriors and political reactionaries alike seek out the like-minded, organize around shared ideas and values, and seek through collective efforts to effect or prevent change in the social or political order.
- 12. It is beyond dispute that individual conduct on social media can pose a challenge to the tenor and sustainability of both polite and democratic discourse. It is true that important voices are lost due to behaviours that would be intolerable in any personal setting: threats of rape, the casual use of abusive language, doxing and multiple other forms of intimidation are rampant in some corners of social media.
  - 13. It is also indisputable that members of certain minorities and affinity groups are singled out for abuse that is vile and threatening: racism, sexism, homophobia, and xenophobia are given voice in ways that intimidate and threaten persons who seek to participate in public discourse.
  - 14. Social media has been and will doubtless continue to be used for both criminal and terrorist recruitment, organizing and planning. Some dark corners of social media are used to facilitate and perpetuate the sexual exploitation of children. The above are all instances of content that the Government styles as Internet Harms –categories that are easily expandable to include further harms.
  - 15. This Proposal, if enacted in legislation, would not and could not lead to a significant reduction in harms or protect vulnerable users of social media.

## The Government's Proposals

- 16. The Proposal identifies five areas of harmful content that are to be subject to a comprehensive regulatory regime. These are:
  - 1. Child exploitation content (including activities that may not be criminal);
  - 2. Content that actively encourages terrorism;
  - 3. Content that encourages or threatens violence;
  - 4. Hate speech as proposed to be defined under amendments to the Canadian Human Rights Act (Bill C-36 of the late Parliament); and,
  - 5. Non-consensual sharing of intimate images
- The five identified harms are not defined in the Proposal: they are merely labels attached to broad categories of expression. It is impossible to comment on the particularities of each harm, as none are defined. The reader is left guessing what the Government intends,

#### Internet Harms

la de la sur l'anné de l'articologieses Estas production inclusion que s

and how far-reaching the ultimate definitions may prove to be. Once the Government has left behind the definitional constraints and the procedural protections of the criminal law, *there is no known limit to the mischief that may be done to speech rights in the name of protecting the vulnerable.* 

- 17. It must be observed that the proposed scheme is one of universal application: it operates without respect to Canadian borders. A social media platform on which the harmful content is posted need have no connection to Canada. It need not have facilities in Canada or receive revenues from Canada or have Canadian subscribers. The scheme applies to content that is considered harmful but that has no connection to either Canada or Canadians. Nor must the content have been expressed in a language that is spoken in Canada. Nor need the person whose speech is at issue have any connection to Canada.
- 18. In short, the Proposal would have Canadian law apply to entities that have no connection to Canada, to speech that has no connection to Canada, and impose remedies for harmful speech for which there is no evidence of harm in Canada. No consideration appears in the Proposal to conflicts between Canadian and foreign domestic law, or what the implications to Canadians might be if foreign governments were to adopt regimes that assumed a similar universal jurisdiction approach.
- 19. The remedies proposed by the Government effectively create two parallel regimes, both of which are intrusive of the privacy rights of individuals. They are designed to chill speech.
- 20. The prime remedy for Internet harms, as proposed by the government, is a mandated censorship regime. It would require social media platforms under the supervision of the state, to censor the speech of their users. The platform-censorship regime would be backed by an ongoing governmental surveillance of the censorship practices of the platforms to ensure they meet minimal government standards and what the government determines to be best practices.
- 21. The second remedy consists of requirements that platforms report to law enforcement and national security agencies content that it may have adjudged harmful under its internal censorship policies.
- 22. Notably, neither remedial regime addresses Canadian domestic speech as such. Each is to be applied to speech wherever it was expressed and in whichever language the impugned speech was expressed.

## The Censorship Regime

23. The Government's proposed response to the challenges posed by the abusive conduct of some social media participants is to impose on social media platforms that are accessible in Canada (as virtually all are in an open Internet) a wide-ranging obligation to censor the

4

The second secon

content, including lawful content posted by their users (which the Proposal euphemistically refers to as content moderation).

24. The Proposal lists five categories of harm, and while those harms are based on criminal law definitions and concepts, the Proposal suggests that they should be moulded to a regulatory context (by which is meant broadened from its narrower criminal law meaning). The Cabinet (Governor in Council) is to be given the power to further define specific terms that constitute elements of the harmful content, so the statutory definition of those Internet Harms would be subject to alteration over time and susceptible of change without further consideration by Parliament.

#### **Platform-Internal Censorship**

- 25. The censorship regime is to apply to social media platforms. However, the Proposal does not define what constitutes social media and in reality the various forms of social media vary enormously from one another. And, it should be noted, Internet services evolve rapidly in ways that may render the approach sketched out in the Proposal meaningless. It is unclear whether the Proposal would capture platforms such as the New York Times or Global TV. There are serious doubts that YouTube is a social media platform. Simply giving Cabinet the power to expand and redefine to whom the proposed legislation is to apply is not the same as having a principled approach to the regulation of social media.
- 26. The censorship regime requires that social media platforms take all reasonable measures (including automated artificial intelligence systems) to identify harmful content and render that content inaccessible to persons in Canada within 24 hours. The manner of rendering impugned speech inaccessible is to be prescribed by Cabinet.
- 27. Social media platforms are to ensure that their private censorship regimes do not result in differential treatment of any group on a ground prohibited by human rights legislation or as may be further prescribed by Cabinet. How this is to be done if the systems used by the platforms are objective is left to the imagination. The Proposal suggests that harmful speech by members of groups protected by human rights legislation is to be judged by a different standard from those of members of groups that are not singled out for human rights protections. How the platforms are to make such decisions are not explained in the Proposal. It is fair to ask how a social media post would know that otherwise harmful content originates from a member of a protected class? This aspect of the Proposal is fundamentally and deeply illiberal in concept, and would be so in implementation.
- 28. If objectionable content evades the platform-internal censorship regime, that speech may be subject of a complaint from a member of the public (not restricted to complaints from Canadians). Once the content has been flagged by a complainant, the platform must, within 24 hours, decide whether to render the content inaccessible to persons in Canada.
- 29. The decision whether to censor the content must be conveyed to the complainant and (though this is not clearly spelled out) to the person who posted the content. They are to

5

(a) A has form by dividualities and properly allocation of our analysis.

have an easy-to-use opportunity to have the decision promptly reviewed and reconsidered. The Proposal does not mention providing an opportunity for an exchange of competing views by the complainant and the content poster. It is hard to contemplate a serious back-and-forth within a 24 hour timeframe.

30. A platform is to establish clear (as prescribed by the Digital Safety Commissioner) censorship (content moderation) guidelines that are to be publicly available.

## **Digital Recourse Council**

- 31. When the platform's internal review mechanisms are exhausted, the complainant or the person who posted the content can appeal the platform's decision to a Digital Recourse Council, composed of 3 to 5 persons appointed Cabinet. Its members are to be subject matter experts reflective of the Canadian population but particularly inclusive of women, Indigenous Peoples, members of racialized communities, religious minorities, LGBTQ2 and gender diverse communities, and persons with disabilities.
- 32. The Council is to issue decisions on whether the content is harmful. If it is found harmful, the Council orders the content be rendered inaccessible to persons in Canada. If it is not found harmful, it will be for the platform to decide whether to suppress the content based on its internal policies.
- 33. There is no appeal of a decision of the Council. A person who disagrees with a Council decision would have to seek judicial review.
- 34. The Council is to provide a copy of the inaccessibility order to the Digital Safety Commissioner, who has the power to ensure that the order is implemented as directed.

## **Digital Safety Commissioner**

- 35. The Digital Safety Commissioner, to be appointed by Cabinet, is basically responsible for ensuring that the platform-internal censorship regimes are functioning, up-to-date, and achieving the desired results (suppression of harmful content). The Commissioner can make regulations applicable to the internal censorship regimes, applying different standards of stringency to platforms based on factors such as size, revenue and business model. The Commissioner can conduct inspections without the necessity of a warrant (given the unsatisfactory definition of to whom the legislation would apply, this could be a serious intrusion on captured businesses). He will have the poser to conduct audits, and to launch incident investigations. The Commissioner will have the power, with judicial authorization, to search private dwellings.
- 36. Where a platform fails to meet its censorship obligations, the platform may negotiate with the Commissioner a compliance agreement that ensures that it corrects any deficiencies in its censorship processes that are of concern to the Commissioner.

- 37. As an alternative, where an agreement is not reached, the Commissioner can issue compliance orders to platforms that fail to meet prescribed standards. A platform can appeal a compliance order to the Personal Information and Data Protection Tribunal (the "Tribunal") a creature of the proposed *Digital Charter Implementation Act* Bill C-11 of the late Parliament).
- 38. Both compliance agreements and compliance orders are legally binding, and breaches can be the subject of either administrative law or criminal law sanctions.
- 39. The Commissioner can recommend that an administrative monetary penalty ("AMP") be imposed on non-compliant platforms. The actual decision to impose an AMP is to be that of the Tribunal, which is to have the power to levy AMPs of up to \$10,000,000 or 3% of the platform's *gross* global revenue (whichever is the greater).
- 40. Where the Commissioner decides not to recommend the imposition of an AMP, a complainant will have the right to appeal that decision to the Tribunal, which may decide to impose an AMP overriding the position taken by the Commissioner. The Proposal does not lay out an obligation on the Commissioner to notify complainants of the results of their investigation. Presumably some such obligation will be included in any forthcoming obligation.
- 41. It is proposed that breaching either a compliance agreement or a the terms of a compliance order will be offences and punishable by maximum fines of \$25,000,000 or 5% of gross world revenues.

## **Advisory Council**

- 42. It is proposed that there be an Advisory Council, whose members would be appointed at the pleasure of the Minister.
- 43. The Advisory Council would not advise the Minister, but rather advise the Commissioner and the Council. The description in the Proposal is too sketchy to ascertain what the Advisory Council might be expected to offer to the Commissioner – who is a law enforcement officer, or to the Council – which is surely expected to bring its independent expertise to bear in making its determinations.

## **Digital Safety Commission**

- 44. It is proposed that a Digital Safety Commission be established. There is very little explanation of what it's function is to be apart from supporting the Commissioner and the Council.
- 45. The Commission is to be headed by a Cabinet appointee, so accountability issues immediately arise. Is the Commission to control the budget and staff of the Commissioner and the Council? Who makes decisions as to the allocation of resources?

7

n de la sur l'activa de la constantinon Altre operationes activas de la constante la sur la constantinon de la constante

What if the Commissioner and the Council are competing for the same resources? The Proposal has no answers to any of these questions.

46. The Proposal is that the Commissioner will make regulations as to charges the regulated entities must pay to cover the costs of the Commissioner, the Council, and the Commission. No estimate is given as to the cost of proposed scheme, nor is it suggested how the burden will be distributed among the various classes of regulated entities.

## The Law Enforcement and National Security Regime

- 47. The Government's Proposal is undecided on the approach it seeks to take with respect to law enforcement and national security obligations, which complicates the analysis of this aspect of the Proposal. The Proposal suggests two alternatives:
  - 1. Social media platforms will be obligated to *notify* the RCMP where the platform has reasonable grounds to suspect that content that it considers to encompass one of the five harms reflects an imminent risk of harm to any person or property (Cabinet is to be given the power to elaborate by regulation); or
  - 2. A platform be will required to *report* to law enforcement information in respect of speech that may constitute a criminal offence (both to be prescribed by Cabinet in regulations) that fall within the five categories of harmful content.
- 48. It is unclear why these measures are posed as alternatives.
- 49. The details of the content of the notifications or reports, their format, and guidance on what constitutes the threshold for these obligations would, again, be left for Cabinet to prescribe by regulation.
- 50. It is also proposed that a platform be obligated to report to CSIS information concerning persons who have posted content that the platform has rendered inaccessible due to its judgment that the post had terrorist content or content that incites violence.
- 51. It is further proposed that a platform be required to retain data and information that are relevant to reports or notifications it has made, the specific requirements of which are to be prescribed by Cabinet.
- 52. In addition, a platform is to preserve data and information about *potentially* illegal content that falls within any of the five categories of harm. Given that all the five harms are based on (if expanded from) criminal law offences, it is hard to see how a platform could fail to retain data and information respecting every instance where it has rendered content inaccessible to persons in Canada.
- 53. Under the Proposal, a platform would not be permitted to disclose that it has issued a report or a notification or disclose the contents of the report or notification if the

#### Internet Harms

la (1917) interferindia de la contractione Referencia de la contraction de la contraction de

disclosure *could* prejudice a criminal investigation – even if a criminal investigation has not begun. The working assumption would have to be that any disclosure would prejudice a criminal investigation, so persons whose personal details have be reported to law enforcement would have no means of counteracting a false implication of wrongful conduct.

- 54. The Proposal would also oblige the platform to take all reasonable measures to ensure that its reports or notifications do not result in the differential treatment of any group based on prohibited ground of discrimination under the *Canadian Human Rights Act* or the regulations. It is difficult to understand how, if the criteria used in assessing harmful content is objective, this provision would be either necessary or just.
- 55. It would be for the Digital Safety Commissioner to oversee the implementation of the proposed law enforcement and national security obligations by social media platforms.

# **ISCC Response**

## **ISCC Principal Critiques**

- 56. In the following pages, ISCC will provide a more detailed critique of the various aspects of the Proposal. ISCC's principal critiques are the following:
  - The regime as proposed is almost entirely unenforceable, applying as it does to
    entities who conduct no operational functions in Canada. Parliament should not
    enact so elaborate and expensive a scheme when its unenforceability renders the
    legislation purely symbolic or worse a charade. While major platforms may
    voluntarily comply with the prescriptions of the regime, the true outliers who
    deliberately voice harmful content will remain outside the reach of Canadian law.
  - 2. Virtually the whole of the proposed legislative scheme would have purely extraterritorial effect. It is hard to understand how Parliament can assume universal jurisdiction over content posted on the Internet that has no link to Canada apart from the fact that Canadians may access that content.
  - 3. The proposed legislative scheme is contrary to the guarantees of free speech enshrined in the *Canadian Charter of Rights and Freedoms* as it applies to lawful speech. The Charter protects not only the expressive rights of Canadians but the right of Canadians to access the expression of others. The Proposal, on its face, violates those rights.
  - 4. The timeframes for platform censorship decisions are so compressed as to compromise the quality and thoughtfulness of platform-internal decisional processes. The objective on any legislation dealing with harmful speech should be to ensure that the right decision is made not just any decision.

- September 25, 2021
- 5. The powers that the Proposal would confer on Cabinet are an affront to our Parliamentary system. As proposed, Cabinet would have both the power to unilaterally mould the definitions of harms and to extend the entities to which the legislation would apply. The proposed power to direct the Digital Safety Commissioner in their enforcement activities are and should be rejected out of hand. The powers that the Proposal arrogates to Cabinet are ones that should only be enacted through Parliament.
- 6. The proposed harms are too diverse to be treated within the same regime. To have this variety of content being judged by the members of a single Council no matter how well qualified its members may be is unfair to the seriousness of the task at hand and the need for the application of expertise to intrinsically complex decision making.

# The Enforceability of the Regime

- 57. Virtually all social media platforms that are routinely accessed by large numbers of Canadians are foreign based. They do not typically conduct their core communications functions in Canada. They may havelimited physical premises and employees in Canada: mostly for marketing and sales. Most of them do not charge subscription fees for access to their platforms, so there are no Canadian user revenue streams to the platforms. The cost of recouping the additional costs of the proposed regime will fall on Canadian businesses who advertise on social media platforms. Doing business in Canada becomes more expensive a drag on Canadian entrepreneurs.
- 58. In terms of the enforcement of the regime over foreign based entities, it would appear that compliance with Canada's internet harms regime will be voluntary: there no principle of comity or conflict of laws that would require a foreign court to recognize Canadian issued inaccessibility or compliance orders, support the payment of fees to sustain the Canadian internet harms administrative apparatus, enforce payment of any administrative monetary penalty imposed by the Personal Information and Data Protection Tribunal, or require a platform to pay fine levied in a criminal prosecution.
- 59. In short, the proposed Internet harms legislation would be a kind of legal Potemkin village. It would look like a stringent and elaborate regime that provides remedies for a persons who are aggrieved by their mistreatment and abuse from harmful content on social media. However, behind the façade of a comprehensive and binding legal regime, only voluntary adherence by social media platforms will give any effect to the regime. The powers will be illusory because they are unenforceable.

- 60. Failure to comply with the legislation, or to obey orders issued by the Digital Safety Commissioner or the Digital Recourse Council, or, indeed, to pay administrative monetary penalties imposed by the Digital Privacy and Data Protection Tribunal may cause a platform reputational harm (or not!) but the legal consequences will be nugatory.
- 61. ISCC believes that Canadian legislation should address the behaviours of Canadians on social media platforms, and seek to create remedies that can be enforced within the Canadian legal system.

# **Extraterritorial Application**

- 62. The Proposal would have social media platforms, wherever located, apply Canadian internet harms legislation to all content wherever and by whomever created, and in whatever language it is posted. The Proposal would have the legislation apply to harmful content that is accessible to persons in Canada. It is not restricted to persons posting content in Canada, or Canadians posting content on a platform, or content that is connected to Canada in some obvious way such as by singling out a Canadian in content that constitutes an Internet harm.
- 63. There are approximately 1,800,000 Chinese born Canadians. Many maintain family, cultural and business ties to China. Western social media platforms are forbidden from operating in China. China has a number of domestic social media platforms having millions of subscribers. Canadians can access those platforms. Those platforms would fall within the scope of the regulated entities under the Proposal. Does anyone truly believe that WeChat or Sina Weibo will pay fees to sustain the Canadian regulatory regime or heed an inaccessibility order issued by the Digital Recourse Council? The answers to those question are self-evident and illustrate the extreme ambition and the true scope of the Proposal's overreach.
- 64. The major social media platforms are not located in Canada. They may not have any facilities in Canada. The computers on which they store data will, in most cases, be located outside Canada. Apart from the laws of their jurisdiction of incorporation or organization, they may subject to the laws of a number of jurisdictions for a variety of purposes, including privacy, data security, criminal law, and laws respecting the protection of personal and institutional reputations. The Proposal would have these platforms conform in the minutest detail to the prescriptions of Canadian law. It would apply Canadian law to censor content posted by persons who have no connection to Canada and whose content does not concern persons located in Canada.
- 65. If a Brazilian posts on Facebook, in Brazilian Portuguese, content that is potentially hateful about Amazonian indigenous peoples, the Proposal would require that the platform make that material inaccessible to Canadians. It would require the platform to notify the Brazilian contributor that it has censored the content and that the decision can

and a second sec

be appealed to the Digital Recourse Council (which, it can be assumed, will operate only in French and English). If the platform fails in that duty, the Digital Safety Commissioner can investigate that omission and, if the platform does not enter into a Compliance Agreement, issue a Compliance Order requiring the platform to remedy the omission. If the platform does not comply, the Digital Safety Commissioner may recommend to the Tribunal that an administrative monetary penalty be imposed, or seek to prosecute the platform for offences that carry fines of up to \$25,000,000 or up to 5% of gross global revenues – whichever is the greater.

- 66. The law enforcement and national security reporting/notification requirements would create requirements that would prove impossible to fulfill. Under the Proposal, every post in every language, wherever in the world it has been given expression, whose content might, if said in Canada constitute a Canadian offence, would be subject to mandatory reporting/notification requirements. Canadian law enforcement and national security agencies could be overwhelmed with notifications respecting content that has no material connection to Canada. It could lead to Canadian law enforcement missing important threats to Canadian interests due to the flood of notifications concerning extraterritorial conduct that will be received from social media platforms. Again, the Proposal does not address the implications of other jurisdictions imposing comparable obligations resulting in the compilation of the personal information of Canadian in foreign police and national security databases. The Proposal is bereft of any consideration of the implications of the Canadian regime for similar conduct by other nation states.
- 67. In some cases, the mere reporting of personal information to Canadian law enforcement or national security authorities may violate the privacy laws of jurisdictions such as Europe that may have a greater connection to the alleged harm and jurisdiction over the person whose information is to be reported to Canadian authorities.
- 68. At the same time, the platform would be required to keep information and data respecting the person posting the content for a period prescribed by Canadian law. This is extreme overreach. It surely violates the privacy interests of large numbers of foreign citizens whose only crime will have been to have come close to expressing words that could be an offence if expressed in Canada.
- 69. A further consideration is that some content that may appear hateful, or suggest an imminent risk of violence or harm to property may come from persons attempting to throw off oppressive governments. Do we really want to be responsible for what happens to oppositional figures if our preservation requirements lead to their personal information falling into the hands of the secret police?
- 70. A certain humility is necessary when Canada attempts to take on the role of policing all harmful speech everywhere in the name of protecting the sensibilities of Canadians.
- Any legislation on Internet harms should be restricted to content that has some meaningful connection to Canada and Canadians.

тер от на Россиру в Уванатания Породној относто се ососното и

72. ISCC recommends that any Canadian legislation to deal with harmful content on the Internet should be developed in cooperation with other democratic states. Only concerted international action can be expected to have prospects of success in suppressing truly harmful content on the Internet.

## **Censorship Regime**

- 73. While it is laudable that the Government seeks to protect vulnerable persons and groups from harmful content, the state imposition of an obligation upon private sector actors to permanently screen and censor the expression of private citizens is wholly unprecedented.
- 74. At present, social media firms tend to have some form of content standards all of which cover the same ground (and much more!) as those targeted in the Proposal. What is new is the decision by the Government to assume direction of the content moderation programs of the platforms.
- 75. The Proposal would seem to render the platforms agents of the state to the extent to which they act in obedience (as they will legally required to do) to the strictures of the law and its administrative apparatus. It is an open question as to whether the Canadian government may render itself liable for the results of good faith measures taken by the platforms to comply with the various elements of the censorship regime including over-zealous application of the identified harms to legal content.
- 76. The regime carries very significant resource implications. Its implementation will require private sector actors to create, redesign, or at least reconfigure, automated artificial intelligence systems for the Canadian market. It will also impose an obligation to engage sufficient human resources to review, assess and respond to flagged content. Given the scale of social media, this obligation would be immense. It is estimated that 720,000 hours of video are uploaded to YouTube alone daily. The regime unavoidably creates incentives for anyone, anywhere in the world, who is personally offended by any content to flag it for review. It will not matter is the content meets the harms criteria that government will set. (That criteria will be replete with regulatory language and opaque to individual users and platform moderators alike.) Complaints, valid, pernicious, deliberately false, or spurious, can be expected to proliferate. And this regime would require social media to examine, assess and respond to each and every one within 24 hours. Those costs could only be passed directly or indirectly on to Canadian users. Why should users in other countries pay for such extravagance?
- 77. The censorship regime is designed to favour censorship over freedom of speech.
- 78. No platform will want to face mandatory compliance orders or administrative fines that may exceed its profits. Nor will it want to expend the resources needed to defend the speech of its users, even if it sincerely believes the impugned speech is not harmful. It

will want not to be chastised or held up to public disapprobation for failing to render borderline posts inaccessible. It will face a plethora of sanctions if it fails to suppress speech that is flagged as objectionable. If in doubt, a platform will suppress rather than defend impugned speech. In consequence the regime will censor huge quantities of lawful speech that does not meet the harms threshold. The expressive freedoms of Canadians – both to communicate content and to receive it – will be limited by foreign entities acting under the direction of the Canadian government.

- 79. The regime is stacked against individual Canadians in other ways. As a result of the natural reluctance of platforms to undergo the time and expense of defending user content, the cost of defending flagged speech will fall on individuals who posted the content. They will have to convince the Digital Recourse Council that it the content is not harmful within the complex definitions that are likely to emerge with the legislative scheme. The complaint-driven system will be overwhelmed. Individuals attempting to defend their content will face an agency struggling to keep up with caseload. Decision time will stretch, and decision-making will be hasty. The posters of content will pay the price in terms of the delay in hearing and the quality of decision-making that the system will permit.
- 80. At present, the major social media have guidelines that would capture and eliminate the types of harm that are the focus of the Proposal. The enforcement of the existing guidelines is delegated to computers equipped with AI software and human intervention, often, but not always, by junior in-house or out-sourced staff.
- 81. The algorithms employed by social media platforms already lead to absurdities. For instance, Facebook computers are taught that comparisons between people and animals are harmful. A person posting that "I am as blind as a bat" or saying "You are a silly goose" are apt to find their account suspended for shorter or longer periods of time. Recently, an article critical of the claims of the alleged medical benefits of ivermectin in treating Covid 19 was suppressed because AI could not distinguish between praise and criticism of the medication.
- 82. AI software has a limited grasp of the English (or French) idiom and a total lack of humour. Satire or a joke will alike face the disapprobation of the unschooled and humourless. Anomalous and unjust results are certain to follow.
- 83. The jurisprudence around the five types of harmful content is deep and nuanced. A reading of the Supreme Court of Canada's jurisprudence on hate speech alone leads to no easy application, particularly in the context of a 24 hour take-down requirement. Postings of any complexity, requiring a close reading of the text and some understanding of the context and subject matter, are unlikely to receive the consideration or understanding that they deserve. Again, with the deck stacked in favour of rigid adherence to prescribed standards, there will inevitably be overly generous interpretation of the guidelines leading to the take-down of posts that may be of real value to matters of public

iPolycoperi/ xeletime-a oconominat-i/

controversy and importance. In short, the Proposal reveals a design that ensures a safetyfirst approach by platforms.

- 84. The speed of decision requirement denies the application of solid judgment to the decision of whether flagged content meets the harms test. It neglects the value of sharply conflicting views on matters of public importance. The sanctions that a platform faces in terms of additional regulatory burdens, compliance orders, audits and inspections, and, ultimately, administrative monetary penalties all incentivize a platform to toe the line of least resistance. The true effect of the Proposal will be the suppression of offensive, provocative and contentious speech as opposed to harmful speech.
- 85. Tthe complaint regime, despite the ability of the Commissioner and the Council to reject frivolous complaints, can easily be gamed by trolls and bullies, who will be able to overwhelm both the platform-internal processes and the regime of complaints to the Commissioner and appeals to the Council. The ease of complaint will bury the redress mechanisms, and both social justice trolls and trolls of the reaction will be able to manipulate the complaint system to stymie timely and effective rectification of the erroneous application of the harms tests.
- 86. The Proposal, if enacted into law, would violate the Charter rights of Canadians and render social media platforms agent of the Canadian state in the violation of those rights. The scheme as a whole is aimed at the suppression of speech and cannot be justified in a free and democratic society.

## Who is Regulated?

87. The Proposal suggests that an online Communications Service Provider (OCS) be defined as:

a service that is accessible to persons in Canada, the primary purpose of which is to enable users of the service to communicate with other users of the service, over the internet. It should exclude services that enable persons to engage only in private communication.

88. It is unclear how this would apply to private forums or chat rooms on the Internet. Would it apply to password protected discussions fora on the Internet? Would it apply to message boards provided to students on university campuses or employees in the context of their employment? Would it apply to the comments sections of newspapers and online publications? What about private chat groups on social media? Are messages posted on Facebook that accessible only by friends captured or intended to be captured? The Proposal gives no hint as to the answers to these obvious and fundamental questions.

CHERT REMAINS

## **Expansion of Regulated Entities**

- 89. The Proposal builds in the potential for incremental broadening in the scope of entities to which the obligations to limit speech would apply. and the standards to which platforms are expected to adhere.
- 90. It is unclear to whom the legislation will apply. It is clear that it is intended apply to social media platforms (although those are not defined in the Proposal) and not to private communications, and exempt ordinary telecommunications carrier services. However, the Proposal suggests that Cabinet would have the power, by regulation, to bring into the scope of the legislation communications services that fall outside the scope of social media. This is completely wrong.
- 91. The harms that the Propoal addresses are caused by the *public* communication of harmful content. How then can one justify that Cabinet could, through regulation, extend the legislation to services that offer only *private* communications? This is an extraordinary extension of state control over private expression. It is repulsive to the fundamental concept of free speech. It undermines Parliamentary oversight of governmental action.

## **Expansion of Internet Harms**

- 92. The Proposal sets out a commitment to redefine and hence expand of the categories of speech that are to be considered harmful. The five categories of harmful content that the Proposal seeks to regulate are all derived from criminal law in which their content is (with great difficulty and uncertainty) understood and applied.
- 93. In the first instance, the Government proposes to modify categories of harm to a regulatory environment. How this is to be done remains unclear. The certain result of redefining the harms in regulatory terms is to expand the scope of the harms from their narrower criminal law origins. This removes an important constraint on the government's ability to limit the right to freedom of speech and expands the scope of speech that is to be considered harmful.
- 94. Second, regardless of the definitions to be encapsulated in the implementing legislation, the Proposal would give Cabinet the power, by regulation, to further define specific terms used in the definition of harmful content. In short, the Cabinet, without the approval of Parliament, could mould the basis of the regulatory regime to suit its political purposes.
- 95. The Proposal would enable an increase in the scope of harmful content to cover speech that is lawful but objectionable. This is the whole rationale behind the proposal. It would render lawful speech subject to government prescribed censorship. ISCC adamantly opposes this intrusion into lawful speech.

Conversion of a conversion of the

- 96. No government, of whatever political stripe, should be given the power to redefine a censorship regime to meet its political objectives without Parliamentary scrutiny. This regime is not about the regulation of agricultural products it is about limiting the freedom of speech. The idea of extending the application of the regime by Cabinet must be rejected.
- 97. Third, the regime may be further extended, or its application made stricter, through the proposed power of direction that Cabinet may exercise over the Digital Safety Commissioner.
- 98. The Commissioner's function is primarily one of law enforcement (though it possesses a limited regulation making power). It is an extraordinary innovation to have a law enforcement officer subject to direction by Cabinet. Even if Cabinet would not be able to intervene in individual cases, it is unacceptable that it should be able to give direction to an officer whose prime duty is to enforce the law.
- 99. The Proposal contains no procedural protections against an arbitrary exercise of the power of direction. There is, for instance, no requirement that a direction be submitted to Parliament for committee study. The proposed power of direction should be rejected.

## The Law Enforcement and National Security Regime

- 100. We are left guessing as to what the Government is in fact proposing with respect to the obligations that are to be imposed on social media platforms. To be obliged to notify the RCMP when content seems to constitute a risk of imminent harm is one thing. It is another thing altogether to be required to report to various law enforcement authorities anytime a post seems to *potentially* violate criminal law.
- 101. As the Proposal would broaden the content to be suppressed beyond the criminal law test, it is difficult to understand how content moderators could be expected to know the difference between the regulatory definition of harm and the appropriate criminal law threshold for the underlying offence. Faced with this dilemma, it can be expected that platforms will over-report potentially illegal content to law enforcement and CSIS, and those agencies will both come into possession of an overwhelming amount of information concerning private citizens most of whom will have no connection to Canada while the platforms will be required under Canadian law to preserve information and data for Canadian law enforcement authorities who have no prospect of initiating criminal investigations or prosecutions in Canada.
- 102. The proposed requirements respecting the preservation of data and information are particularly sweeping. A platform would be required to preserve data underlying a report or notification that it is required to make. In addition, and separate from that, a platform is to be required to preserve data and information pertinent to "*potentially illegal content* falling within the five (5) categories of regulated harmful content" (emphasis added). As all the categories of harmful content are based on underlying

#### Internet Harms

CHEVE A REPORT OF A PROPERTY O

criminal offences, it seems clear that *any* content that has been rendered inaccessible to persons in Canada is *potentially illegal*, and thus must be preserved for a period prescribed by Cabinet.

- 103. Cabinet would, under the proposal, be given the power to specify the threshold for what constitutes potentially illegal content. Even were it to do so, it is impossible to think that any guidance from Cabinet would significantly reduce the scope of information and data to be preserved, or reliece a platform from its obligations in a way that would reduce a safety-first approach to data preservation. This represents a significant burden on the resources of the platforms, but more importantly a trove of information and data that could serve as a target for hackers or activists that could be used to compromise the reputation and privacy of individuals whose posted content was, for whatever reason and however unjustly, rendered inaccessible to persons in Canada.
- 104. Again, the pretence to universal jurisdiction claimed by the Proposal will work against the interests of Canadians. The swamping of law enforcement and national security agencies with notifications may actually harm ongoing investigations and overwhelm law enforcement and national security resources.

## **Categories of Harm are too Diverse**

- 105. ISCC agrees that the identified categories pose real harms to society at large, to individuals within identifiable social or minority groups, and to healthy public discourse. However, each harm is very distinct from the others and all demand very different knowledge, experience and understanding to come to grips with. Terrorist recruiting and incitement does not look like rape threats or revenge porn: it cannot be expected that the Digital Recourse Council, as proposed, will be able to effectively deal with such disparate content or harms. The seriousness of the harms merits that each very distinct type of content be considered separately and with the relevant expertise applied.
- 106. ISCC recommends that distinct legislation be considered for each type of harm and their adjudication be based on subject matter expertise rather than by persons whose primary qualification is their affinity for the persons most commonly victimized by harmful content.

## The Administrative Regime

107. The Proposal seeks to create a comprehensive administrative regime involving the creation of new administrative bodies and enhancing the jurisdiction of existing ones. It proposes the creation of unique administrative law remedies. It also proposes to constrain the choice as to who may be appointed to exercise those powers.

The second s

- 108. ISCC believes that the cost and weight of the proposed scheme of administration far outweighs any benefit that may be found in the reduction of harmful content.
- 109. ISCC also believes that the costs of compliance with the proposed regime will stifle any attempt to create domestic social media platforms: this could destroy Canadian creation and Canadian entrepreneurship – and is most likely to have greatest impact in French Canada where unique cultural factors may offer an opening for a genuinely domestic platform.
- 110. ISCC notes with concern the proposal that both the Council and the Advisory Board would, by legislation, emphasize the appointment of persons reflective of groups who are protected by human rights legislation. It may be that such groups are more singled out for abuse than others today – but that in not likely always to be true. It is also critical that if a Council is ultimately created, it should be seen as impartial and not merely to reflect the views of minority communities – as important as those views may be.

## **Other Concerns**

## Constitutionality

111. The constitutional underpinnings of the Proposal need to be examined in depth. There is no head of power that gives Parliament, outside of broadcasting and the criminal law, to control speech.

## **Impact on Advocacy**

112. The regime, if implemented as proposed, may well hamper the ability of victims of child sexual exploitation or revenge pornography to address the substance of their victimhood and educate the public about the facts of these abuses. In effect, the regime could deny real victims a voice.

## News Reporting and Academic Research

113. In seeking to suppress harmful content, the proposed regime could negatively impact the ability of Canadian reporters and academics to access content that is necessary to their work and stifle their ability to express their findings to Canadians. The world is an unattractive place at times, but truth and reality should be addressed head-on. The proposed censorship could have serious unintended negative impacts on news gathering and scholarship.

## Site Blocking

114. It is part of the Proposal that, in exceptional circumstances, the Commissioner could seek an order from the Federal Court to block specific sites. Experience has shown that such orders are ineffective. They do lead to over-blocking. They lead to a perpetual

Let Q and Provide device and a second secon second sec

game of whack-a-mole as objectionable sites relocate and Internet service providers are constantly playing catch up. As well intentioned as site blocking as a remedy may be, the harms they cause and their expense – especially to small operators – suggest that it is not an effective remedy and should not be adopted.

#### Harm to Internet Infrastructure

115. The Proposal to render content inaccessible from Canada is not one that accords with the open Internet and is not compatible with the current structure of the Internet. If effect, the Proposal requires the creation of kill switches to block content from being accessed "by persons in Canada". This latter phrase, which recurs throughout the proposal, would suggest that platforms will have to reconfigure their systems such that Canadians could not reach content by means of virtual private networks or proxy servers. This requires a major investment in blocking work-arounds and restricting Canadian access to the global Internet. The Proposal seems to verge on proposing a great Canadian firewall. ISCC believes this would be both expensive and ineffective. If effective, it would be injurious to Canadian users of the Internet.

# Conclusion

- 116. ISCC asks the Government to drop the Proposal in its entirety. If the Proposal were to be adopted anything like its present form it would represent a serious infringement on the free speech rights of Canadians as guaranteed by the Charter. It would be unenforceable against most of the entities to which it is directed thus undermining the credibility of the regime and of Canada's system of laws. The extraterritorial application of the proposed regime will conflict with the laws of other nations, and harm the privacy and reputational interests of citizens of other countries. The adoption of the scheme would negatively impact the functioning of the Internet in Canada.
- 117. The scheme is unworthy of consideration by Parliament. Its implementation would diminish the rights of Canadians while failing in its purpose of protecting Canadians from Internet harms. The Proposal should be withdrawn.

Separations and the second se second sec

1



## BRIEF SUBMISSION TO THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS: PROTECTION OF PRIVACY AND REPUTATION ON PLATFORMS SUCH AS PORNHUB.

Date: May 14th, 2021

The Ottawa Coalition to End Human Trafficking works to meet the acute, immediate, and long-term resources and support needs of persons impacted by human trafficking, including those who have exited a trafficking situation, their families, and communities, as well as persons who may be at risk of exploitation for the purposes of sexual exploitation, labour exploitation and/or organ removal/harvest. We also provide training to volunteers and service providers to educate them on the indicators of human trafficking, to develop their ability to identify a trafficked person, and to know how to respond appropriately. We are a community-based network made up of various local organizations, service providers and community members from a wide range of diverse backgrounds, both educationally and occupationally. Our approach to human trafficking is a preventative one, focusing heavily on training and assisting survivors.

#### What is our stance?

The coalition has chosen to speak out on the ongoing investigation into Pornhub (and more specifically, Bill S-203) for several reasons. We as a coalition are primarily concerned with how companies like MindGeek and platforms like Pornhub are increasing the demand for child sexual abuse images and, in the long run, are fostering an environment and greater opportunity for human trafficking and sexual exploitation.

After having read the witness testimonies and submitted briefs, we agree that the RCMP's hesitancy to launch an investigation into the allegations against MindGeek is unacceptable and criminal in and of itself. There seems to be some confusion within Canada's national police agency as to whether or not they have jurisdiction to investigate the allegations against MindGeek. In a letter sent to the RCMP Commissioner, Brenda Lucki, the RCMP was called on to recognize the severity and importance of this issue and to launch a full investigation into MindGeek's failure to report child sexual abuse material (Wittnebel, 2021). The letter mentions that Canada's strong child protection laws are only effective "through robust investigation and application by law enforcement" (Wittnebel, 2021). Regardless of the complexities of the task of determining jurisdiction, the RCMP is part of a group of international agencies that are tasked with facilitating such investigations. The RCMP has a duty to protect the victims impacted by the unjust and criminal actions of MindGeek and its video sharing platform Pornhub, to all Canadian children who may be at risk for sexual abuse and/or exploitation, and to the general Canadian population who has placed their trust in this institution to protect Canadians. This is an issue that requires priority, attention, and dedication on all fronts, and thus far has not been treated in this manner by institutions like the RCMP. The victims involved in this investigation and the thousands of other victims out there deserve our greatest efforts and support.

The coalition acknowledges that CSAM and online sexual exploitation has always been a problem, but the COVID-19 pandemic has further exacerbated the issue. The global pandemic

2

has "led to an unprecedented rise in screen time" as families rely on technology to teach, occupy, and entertain their children (UNICEF, 2020). This increased internet usage means a greater likelihood that children will be exposed to pornography and online predators. Regardless of preventatives measures, children are becoming more comfortable and taking more risks online, which means that encountering pornography is almost a guarantee. The issue, as many others have pointed out, is the impact that exposure to pornography can have on children. For children who have no prior sex-education, pornography may be their first and main source of information and answers on the topic (Quadara, El-Murr, & Latham, 2017). An introduction to pornography can easily escalate into a regular habit for children. The coalition fears that the hypersexualization of today's social media, paired with the plethora of easily accessible online sexrelated content, can create a connection to human trafficking. It may seem harmless at first, but over time, exposure to sex-related content and increased interactions on platforms like Pornhub will only increase the demand for such material, and in turn, the demand for human trafficking.

Lastly, the coalition strongly believes in the beneficial and proactive nature of educating the public on the basics, dangers, warning signs and necessary preventative measures and tools to combat the spread of CSAM and human trafficking. The phrase "stranger danger" is still commonly used when educating youth about safety online. In reality, young people are often lured by those they trust - family members, friends, and partners. Educating youth, adults, and those in positions of authority like teachers about the reality of online sexual exploitation and human trafficking will prove to be preventative and work to challenge and dismantle the stigma surrounding the issue.

#### **Recommendations?**

The coalition has several recommendations in response to Bill S-203 An Act to restrict young persons' online access to sexually explicit material. Firstly, the coalition understands sex workers have been at the forefront of making pornographic websites a safe place both for those creating the content and those consuming it. We also understand and appreciate that sex work is a form of harm reduction, and we want to make it clear that we are not calling for the removal of porn. In introducing Bill S-203, the coalition does not wish to infringe upon sex workers' rights; however, significant changes must be made to eradicate CSAM on sites like Pornhub and impede the fostering of human trafficking environments.

Secondly, the coalition recommends a third-party oversight. The companies in question have a vested interest in having such a wide and overwhelming range of content available to its viewers. With a library of millions of videos, pictures, and other forms of content, evidence of CSAM, non-consensual and unverified content on the popular site is certainly evident. Employing a third party to moderate can help to ensure that the content has been thoroughly reviewed, that the acts depicted are deemed consensual, and the age of the creators and those depicted in the content can be properly verified. The third-party must be objective, meaning they have no ties to the company's Pornhub and MindGeek, no ties to the porn and/or sex industry, and are educated with respect to what to look for. This will account for potential bias and will aid in avoiding interests of profit overshadowing the safety of participants and the public.

Thirdly, we recommend that sites such as Pornhub remove all opportunities for content to be shared or downloaded. As we have heard from witness testimony, victims have found it incredibly hard to have their non-consensual or CSAM material taken down. This is partially due to the fact viewers can save, share, download and re-upload content. Taking away a viewer's ability to share or download content will aid in preventing the spread of non-consensual or

3

CSAM material. Removing this feature will not be enough as there are always alternative ways to save and record content without downloading it. For this reason, we recommend porn sites also use software such as Digital Rights Management which protects content from being screen recorded.

Our fourth recommendation relates to the duty to report. The duty to report does not simply fall onto one body or one person. The responsibility to report content that has been published non-consensually, depicts non-consensual acts, or contains evidence of child sexual abuse material should fall on anyone who chooses to visit sites like Pornhub. As much as viewers should be heavily encouraged to report any material suspected to contain CSAM, a greater onus must fall on corporations, creators, and media platforms. These larger bodies have the power, resources, and influence to protect, help and support victims of sexual abuse and exploitation, and they should be held to a higher standard. Additionally, information about how to report and where to report illegal and/or non-consensual content should be easily accessible and advertised to the public. Reports of CSAM should be taken seriously and followed up in a timely manner to reassure victims that their concerns have been heard and are of great importance. Larger companies like Pornhub, MindGeek, Facebook and other media moguls should be held corporately responsible for their failure to report. Not only should these companies face legal punishments for exploiting and profiting from human trafficking material, but the individuals behind the corporate veil should also face the consequences of their actions. The coalition also strongly recommends that the appropriate resources be made available to victims, and that local police forces and the RCMP be adequately trained and equipped to handle these types of cases. We recommend implementing an international task force that can help coordinate and enhance communication between police forces and organizations around the world. Content is often distributed to websites, social media pages, and personal computers and/or cell phones around the world. When the content crosses borders and continents, it causes problems for victims who are trying to get their exploited content removed. An international task force would put an end to some of the international red tape and jurisdictional issues. So many victims and survivors have voiced their frustrations regarding not feeling heard and getting no response from authorities, which is why one of the priorities of this task force must be responding to victims in a timely manner.

Lastly, the coalition sees monumental issues with Bill S-203 section 7 *Defense - Age verification*. The section allows perpetrators of CSAM to escape conviction of the very offenses the Bill is aiming to criminalize. The accused in this case, Pornhub, can implement age verification software, but still fail in preventing someone underaged from accessing content on their website. Simply having this software in place, regardless of whether it works or not, serves as a scapegoat. This clause can easily be misconstrued and used to the advantage of those with deep pockets and influence to avoid punishment and conviction. Clauses like this one are vague, ambiguous, and open to too much interpretation and they will only create more issues in the future. We recommend that such sections be reviewed by third party legal bodies to determine their efficacy, the overall ability to enforce them, and more importantly, whether they can be upheld in court if it comes to that.

We would like to thank the committee for the inclusion of our brief, and we appreciate the opportunity to present our opinions, ideas, and recommendations to the standing committee on this issue. The Ottawa Coalition to End Human Trafficking is hopeful that this investigation will lead to real positive change and offer the victims of human trafficking a sense of justice.

 J CL UP/GODIA 2 PM/IMM/UMU Kicument seemed comprise. HE ACCESS IN MIDIRMARK AICH



LEAF WOMEN'S LEGAL EDUCATION & ACTION FUND FONDS D'ACTION ET D'ÉDUCATION JURIDIQUE POUR LES FEMMES

# Submission to Canadian Heritage on the Federal Government's Proposed Approaches to Address Harmful Content Online

25 September 2021

# Written by: Moira Aikenhead, Suzie Dunn, and Rosel Kim<sup>1</sup>

<sup>&</sup>lt;sup>1</sup> Moira Aikenhead is a PhD Candidate at the Peter A. Allard School of Law at the University of British Columbia. Suzie Dunn is an Assistant Professor at Dalhousie University's Schulich School of Law and is a Senior Fellow with the Centre for International Governance Innovation. Rosel Kim is a Staff Lawyer at the Women's Legal Education and Action Fund. Jane Bailey, Cynthia Khoo, Ngozi Okidegbe, and Karen Segal also contributed to this submission.

(Joda/ment-communique, en initia de la Leti sue l'accela d' reflerencieur Obcument dese sed que que qu' the access de relation de les

# Page 2

# Table of Contents

Introdu	action
About	LEAF and its Expertise
Issues	with the Regulatory Framework from a Substantive Equality Perspective5
Α.	Lack of Substantive Equality Framework6
В.	Lack of Consultation
С.	Overbreadth and Inextricable Connection with the Criminal Justice Process
D.	The Timeframe for Takedown Requirements Must be Tailored for Different Harms. 11
Ε.	Necessity of Transparency and Disaggregated Data from Platforms on All Instances
ofT	FGBV
F.	Issues Regarding a Digital Safety Commissioner
G.	Increasing the Focus on Education and Prevention17
н.	Dangers of Algorithmic Moderation
Appen	dix: Full List of Recommendations from "Deplatforming Misogyny"

# Introduction

The Women's Legal Education and Action Fund (LEAF) supports the development of a federal regulatory framework to address the growing issue of technology-facilitated gender based violence (TFGBV), which disproportionately impacts historically marginalized communities, including women, girls, and gender-diverse people. However, we do not support the federal government's proposed "online harms" framework as drafted, because it poses serious concerns from a substantive equality and human rights perspective and risks exacerbating existing inequalities, particularly because it purports to deal with five very different "online harms" with a single approach.

LEAF believes that in order to deal effectively with the growing issue of TFGBV, the government must allocate resources to create a regulatory framework dealing exclusively with it as a particular harm. We urge the government to: a) revise the regulatory framework to explicitly recognize substantive equality and human rights as guiding principles; b) to provide more immediate and direct support to victims experiencing TFGBV; c) to provide alternative remedies to those provided through law enforcement and the criminal justice process; d) to recognize forms of TFGBV that are not currently captured by the criminal law; and e) to ensure responses are tailored to and account for the specific harms of TFGBV.

#### About LEAF and its Expertise

LEAF is a national, charitable, non-profit organization that works towards advancing substantive gender equality through litigation, law reform, and public education. Since 1985, LEAF has intervened in over 100 cases—many of them before the Supreme Court of Canada that have advanced equality rights in Canada.

Some forms of online harms—as defined by the proposed framework—directly engage LEAF's mandate of substantive gender equality. Conduct such as hate speech and nonconsensual distribution of intimate images (NCDII) have a disproportionately detrimental impact on women and gender-diverse people's ability to express themselves and participate without fear in many online spaces that have become crucial to our professional and personal lives. These harms are the ones we will address in this submission.

LEAF has developed expertise in the gendered impact of online hate and TFGBV. In 2019, LEAF intervened in the landmark case of  $R \vee Jarvis$ ,<sup>2</sup> where it urged the Supreme Court of

2 2019 SCC 10.

Canada to apply an equality lens when interpreting the *Criminal Code* provision of voyeurism. LEAF has also made submissions to Parliament to highlight the gender equality implications of hate speech and online hate, such as its submission to the House of Commons Standing Committee on Justice and Human Rights' study of online hate in 2019.<sup>3</sup> In April 2021, LEAF released a research report <u>"Deplatforming Misogyny"</u><sup>4</sup> by human rights and technology lawyer Cynthia Khoo, which examines how digital platforms can be held accountable and liable for their role in perpetuating TFGBV from a substantive equality perspective.

In "Deplatforming Misogyny", LEAF made 14 recommendations for federal action to regulate TFGBV, including legislative reform. These recommendations are based on 6 guiding priorities that emerged from the research and analysis conducted in this report and should govern efforts to address TFGBV in Canadian law. These priorities are:

- recognizing a need for legal reform to address TFGBV, including through platform regulation;
- recognizing that Canadian constitutional law justifies imposing proportionate limits on freedom of expression in order to uphold and protect the rights to equality and freedom from discrimination, and also to give full effect to the core values underlying freedom of expression;
- 3. guaranteeing that legal reforms that address TFGBV build in victim/survivor-centered, trauma-informed, and intersectional feminist perspectives;
- 4. ensuring expedient, practical, and accessible remedies for those targeted by TFGBV;
- 5. providing due process mechanisms to users who wish to contest platforms' content moderation decisions (whether a decision to leave up or take down content); and
- 6. requiring transparency from platform companies regarding their content moderation policies and decisions, as well as the outcomes of such policies and decisions concerning TFGBV.

<sup>&</sup>lt;sup>3</sup> Women's Legal Education and Action Fund, "Submission to the House of Commons Standing Committee on Justice and Human Rights Respecting the Committee's Study of Online Hate" (2021), online (pdf): *Women's Legal Education and Action Fund* <a href="https://www.leaf.ca/wp-content/uploads/2019/05/2019-05-10-LEAF-Submission-to-the-Standing-Committee-on-Justice-and-Huma....pdf">https://www.leaf.ca/wp-content/uploads/2019/05/2019-05-10-LEAF-Submission-to-the-Standing-Committee-on-Justice-and-Huma....pdf</a>.

<sup>&</sup>lt;sup>4</sup> Cynthia Khoo, "Deplatforming Misogyny" (April 2021), online (pdf): *Women's Legal Education and Action Fund* <<u>https://www.leaf.ca/publication/deplatforming-misogyny/</u>>. [*Deplatforming*]

Of LEAF's fourteen recommendations for federal action, we emphasize the following six that are relevant to our submission (see the <u>Appendix</u> of this submission or the <u>"Deplatforming Misogyny"</u> report for full list):

- Establish a centralized expert regulator <u>for TFGBV specifically</u>, with a dual mandate:

   a) to <u>provide legal remedies and support to individuals</u> impacted by TFGBV on digital platforms, including regulatory and enforcement powers; and b) to develop research on TFGBV and <u>provide training and education to the public, relevant stakeholders, and professionals</u>.
- Ensure that legislation addressing TFGBV integrates substantive equality considerations and guards against exploitation by members of dominant social groups to silence expression by members of historically marginalized groups.
- Ensure that <u>legislation to address TFGBV focuses solely on TFGBV (including intersectional considerations)</u>—do not dilute, compromise, or jeopardize the constitutionality of such legislation by 'bundling' TFGBV with other issues that the government may wish to also address through platform regulation.
- Enact a law that allows for victims/survivors of TFGBV to obtain <u>immediate removal of</u> certain clearly defined kinds of content from a platform without a court order, such as the non-consensual distribution of intimate images.
- Require platform companies to undergo independent audits (which could be conducted by the new TFGBV agency) and <u>publish comprehensive annual</u> <u>transparency reports</u>.
- Fund frontline support workers and community-based organizations working to end, and supporting victims/survivors of, gender-based violence, abuse, and harassment, specifically to enhance their internal expertise, resources, and capacity to support those impacted by TFGBV (which often accompanies genderbased violence and abuse).

### Issues with the Regulatory Framework from a Substantive Equality Perspective

It is LEAF's view that regulating hateful, discriminatory, and harmful content is necessary and important for enhancing freedom of expression and equality rights. LEAF also believes that the government must play a central role in regulating TFGBV, because technology companies that operate digital platforms have not demonstrated willingness to safeguard the rights of free expression for <u>all</u> users. In fact, recent investigations into business decisions of digital platforms demonstrate how the companies are ignoring the evidence of harm that users

experience, because online hate and harassment can be particularly lucrative.<sup>5</sup> It is therefore inadequate to leave the work of regulating profitable, yet harmful, online content, including many forms of TFGBV, to the very companies who stand to gain from that content. These realities underscore the broader need for regulation of industry practices that themselves incentivize and perpetrate online hate, harassment and discrimination. The government has a crucial role to play in prioritizing Canadians' constitutional rights over corporate growth. In order for the regulatory framework that addresses TFGBV to be effective, it must be grounded in substantive equality and human rights.

For the reasons cited above, we encourage a governmental regulatory framework including an expert regulatory body—which we believe is necessary for protecting the freedom of expression and equality rights of all, especially for women and gender-diverse people. However, the proposed regulatory framework is inadequate and raises several concerns from an equality perspective. Our comments will focus on the types of online harms included in the framework that LEAF has expertise in: hate speech and NCDII. We will also include some comments on child sexual abuse material (CSAM).

As explained below, we find it highly problematic that such distinct harms as NCDII would be addressed under the same legislation as other offences such as terrorism, and believe each of the harms the framework proposes to address require unique approaches and considerations.

We outline our concerns in detail below:

A. Lack of Substantive Equality Framework

Any regulation of hateful or harmful speech <u>must adopt an explicitly intersectional</u> <u>and substantive equality lens</u>.<sup>6</sup> It must recognize that discriminatory, threatening and other harmful speech targets and silences marginalized voices.<sup>7</sup> Research in Canada and abroad show that when women and other marginalized groups are faced with discriminatory and hateful speech, non-consensually distributed images, and attacks when speaking out about

<sup>&</sup>lt;sup>5</sup> Georgia Wells, Jeff Horwitz and Deepa Seetharaman, "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show", *Wall Street Journal* (14 September 2021), online:

<sup>&</sup>lt;<u>https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=article\_inline>.</u>

<sup>&</sup>lt;sup>6</sup> Deplatforming, supra note 4 at 222-223.

<sup>&</sup>lt;sup>7</sup> See Saskatchewan (Human Rights Commission) v Whatcott, 2013 SCC 11 at para 114.

equality issues, one of the main consequences is for the targeted groups to engage less or to stop engaging online.<sup>8</sup>

Adopting substantive equality principles requires acknowledging the ways regulatory frameworks and content moderation processes can be abused by dominant groups to further silence marginalized voices.<sup>9</sup> Beyond silencing marginalized voices and forcing members of these groups offline, hateful online rhetoric has resulted in significant tangible harms and violence to these groups. Hateful and discriminatory online speech has been connected to some of Canada's deadliest attacks including the Toronto van attack and the Quebec City mosque shooting where the attackers had a history of following sexist online groups, (incels) who promote violence against women and hateful Islamaphobic online groups, respectively, prior to their attacks and posting sexist and racist content online.<sup>10</sup> The focus of regulating TFGBV in digital spaces must centre squarely on the abuse of historically marginalized groups, advancing their equality and upholding their human rights.<sup>11</sup>

<u>The government must commit to addressing hateful speech and violence</u> <u>targeting these equality-seeking groups by making this intent explicit in the regulatory</u> <u>framework, and the substance of the framework should reflect that intention</u>. The framework proposed in the Technical Paper acknowledges that online hate has disproportionate impacts on marginalized groups including women, Indigenous Peoples, members of racialized and religious minority communities and LGBTQ2 and gender-diverse communities and persons with disabilities. It is ostensibly premised on respecting and protecting the ability of people to fully participate in the public discourse free from harm.<sup>12</sup>

The regulatory framework requires Online Content Service Providers (OCSPs) to ensure that the implementation of measures to make harmful content inaccessible does not

https://journals.sagepub.com/doi/full/10.1177/1473779521991557>.

<sup>&</sup>lt;sup>8</sup> See Amnesty International, "Toxic Twitter - A Toxic Place for Women" (March 2018) online: Amnesty International <a href="https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-1/">https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-1/</a>; Anastasia Powell & Nicola Henry, Sexual Violence in a Digital Age (London: Palgrave Macmillan UK, 2017); Plan International, "Free to be Online? A report on girls' and young women's experiences of online harassment" (October 2020) online: Plan International <a href="https://plan-international.org/publications/freetobeonline">https://plan-international.org/publications/freetobeonline</a>>.

<sup>&</sup>lt;sup>9</sup> Deplatforming, supra note 4 at 224.

<sup>&</sup>lt;sup>10</sup> Stephane J Baele, Lewys Brace & Travis G. Coan, "From 'Incel' to 'Saint': Analyzing the violent worldview behind the 2018 Toronto attack" (2019) Terrorism and Political Violence, DOI: <u>10.1080/09546553.2019.1638256</u>; Michael Nesbitt, "Violent crime, hate speech, or terrorism? How Canada views and prosecutes far-right extremism (2001-2019)" (2021) 50:1 Common L World Rev 38 <</p>

<sup>&</sup>lt;sup>11</sup> Deplatforming, supra note 4 at 225.

<sup>&</sup>lt;sup>12</sup> Government of Canada, "Technical Paper" (29 July 2021) at 1.c.; 1.h, online: *Canadian Heritage* <a href="https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html">https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html</a>. [*Technical Paper*]

Page 8

"result in differential treatment of any group on a prohibited ground of discrimination."<sup>13</sup> Once again, the government must explicitly acknowledge and name what groups are likely to be targeted and adversely impacted by TFGBV, and guarantee that any measures to identify and render inaccessible harmful speech must not operate to silence voices that have been historically marginalized. Research has shown that women and gender-diverse people, particularly those with intersecting marginalities such as race, sexual orientation, gender expression and disability face increased online attacks based on their identity and often respond to these attacks by engaging less online.<sup>14</sup>

#### B. Lack of Consultation

Despite some communication with organizations and individuals with expertise on TFGBV, the Government failed to consult meaningfully with experts, civil society groups, victims and survivors of TFGBV in crafting the proposed framework. To the extent that the government held consultations and conversations with a select group of organizations and individuals (as it did with LEAF), the current proposal does not reflect many of the recommendations or concerns that were raised. For example, LEAF raised concerns about the extensive information-sharing powers that were proposed during a joint call with Feminist Alliance for International Action (FAFIA) and Heritage staffers on February 10, 2021. It also raised concerns about the focus on criminal law enforcement and encouraged the government to take a substantive equality approach to this legislation.

In order to ensure any proposed legislation does not result in unintended adverse consequences for equality-seeking groups, the government must meaningfully consult with groups and organizations with specialization in these areas before tabling any proposed legislation governing the regulatory framework, Digital Safety Commissioner, or Digital Recourse Council of Canada and Advisory Board. We understand the Liberal Government intends to introduce legislation governing online harms within its first 100 days.<sup>15</sup> We strongly caution against such an approach as a significantly more robust and meaningful consultation with impacted groups is required, which is not possible in the proposed 100-day timeline.

<sup>13</sup> Ibid at 10.a.

 <sup>&</sup>lt;sup>14</sup> See Amnesty International, "Toxic Twitter - A Toxic Place for Women" (March 2018) online: Amnesty International < https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-1/>.
 <sup>15</sup> Liberal Party of Canada, "Forward. For Everyone: Protecting Canadians from Online Harms." (2021), online: Liberal <a href="https://liberal.ca/our-platform/protecting-canadians-from-online-harms/">https://liberal.ca/our-platform/protecting-canadians-from-online-harms/</a>.

#### C. Overbreadth and Inextricable Connection with the Criminal Justice Process

Like other forms of gender-based violence, TFGBV is rooted in intersecting and systemic oppressions including misogyny, racism, colonialism, homophobia, transphobia and ableism.<sup>16</sup> It is crucial that legislation aimed at addressing TFGBV explicitly focus on TFGBV specifically, and not conflate it with other forms of "online harms". While there is an urgent need to address other forms of what the framework has defined as "online harms", it is inappropriate to conflate these distinct issues under one single approach. "Bundling" regulation of this form of TFGBV with other types of content moderation, such as speech related to terrorism, compromises the utility and integrity of such a framework, and jeopardizes its constitutionality.<sup>17</sup>

By proposing to regulate five separate and distinct categories of harmful content (child sexual exploitation; terrorist content; content inciting violence; hate speech; and the nonconsensual distribution of intimate images), each of which requires its own unique response, the proposed framework is overbroad and prevents the specified tailoring needed to adequately respond to each of these unique issues. Each of the "online harms" identified in the framework must be addressed individually, particularly when it comes to reporting mandates, types of support available for victims, and the necessity and timing of content removal.

The five categories of harmful content covered by the framework are each subject to the provisions of the *Criminal Code*.<sup>18</sup> While the definition of "hate speech" is to be informed by the definition under the *Canadian Human Rights Act*, the hate speech provisions under that legislation are not yet in force, and the proposed definition closely mirrors the interpretation of "hate propaganda" pursuant to the *Criminal Code*.<sup>19</sup> While the framework suggests definitions must be adapted to the regulatory context, it is not clear what this means.<sup>20</sup> This framework should develop definitions of TFGBV that are grounded in substantive equality, rather than the criminal law, which has not always centered gender equality.<sup>21</sup> The

<sup>20</sup> Technical Paper, supra note 12 at 8.

<sup>21</sup> See e.g.: Emma Cunliffe, "Sexual Assault Cases in the Supreme Court of Canada: Losing Sight of Substantive Equality?" (2012) 57 SCLR (2d) 295 < <u>https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2111652</u>>; Margaret Denike, "Sexual Violence and 'Fundamental Justice': On the Failure of Equality Reforms to Criminal Proceedings" (2000) 20:3 Canadian Woman Studies 151 <</p>

https://cws.journals.yorku.ca/index.php/cws/article/viewFile/12681/11764>.

<sup>&</sup>lt;sup>16</sup> Deplatforming, supra note 4 at 225.

<sup>17</sup> Ibid at 228.

<sup>&</sup>lt;sup>18</sup> Criminal Code, RSC 1985, c C-46.

<sup>&</sup>lt;sup>19</sup> Bill C-36, *An Act to amend the Criminal Code and the Canadian Human Rights Act and to make related amendments to another Act (hate propaganda, hate crimes and hate speech)*, 2nd Sess, 43rd Parl, 2020-2021 (first reading 23 June 2021).

framework's definitions must emphasize the need to regulate content that interferes with the equality rights of those targeted by the content. For example, the framework should target forms of TFGBV targeting women, girls, and gender-diverse people.

The framework represents a missed opportunity to provide support to victim/survivors of TFGBV by failing to address some of the most common forms of problematic content online that does not meet the definitions set out in the Criminal Code, but still causes significant harm. For example, rape threats and death threats are frequently aimed at equality-seeking groups, however, many of these threats may not reach the criminal definition of uttering threats. It should also be noted that many forms of TFBGV that proliferate online were not included in the list of "online harms", such as harassment and threats. It is not clear why the five specific harms were selected for regulation and not others. Further, criminal definitions of hate speech and NCDII cast a fairly narrow net, excluding many kinds of hateful online commentary and exploitative images that do not fit in the definitions within the Code. Content that does not rise to the level of criminality can still cause serious harm to marginalized groups.<sup>22</sup> The government must provide mechanisms to support groups targeted by content that does not meet the definition of criminality but is nevertheless harmful, such as providing support in navigating social media's content moderation procedures and providing emotional and technical support, particularly if that content breaches a platform company's own content moderation rules.

Aligning the definition of "online harms" with Criminal Code offences, and requiring mandatory reporting to law enforcement in certain circumstances, does not align with a victim/survivor-centric, intersectional, or substantive equality approach to regulating TFGBV. Victims/survivors should have some element of choice when seeking support. For some, this may involve a criminal justice response, while others will be better served through less formal support, such as a government help line or victim service support workers providing technical and emotional support. Members of marginalized communities that have a history of being over-criminalized or having their complaints ignored or neglected by the police. Particularly, Black, Indigenous, and racialized communities, and women reporting sexual violence, may be reluctant to engage in a regulatory system that requires reporting to the police due to factors such as over-criminalization, even if the content they are concerned with is criminal in nature.

In cases involving TFGBV such as NCDII, <u>LEAF recommends that there can be no</u> mandatory reporting to law enforcement without the express informed consent of the

<sup>22</sup> The United Kingdom, Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department, "Online Harms White Paper" (April 2019), online (pdf): *GOV.UK* 

<sup>&</sup>lt;a href="https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/973939/Online\_Harms\_White\_Paper\_V2.pdf">https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/973939/Online\_Harms\_White\_Paper\_V2.pdf</a>

<u>victim/survivor</u>.<sup>23</sup> Mandatory reporting may be appropriate and required under existing legislation for cases involving child sexual abuse material. For adult women, a mandatory reporting regime may deter some from seeking help because not everyone wishes to engage the police. While police involvement may be necessary in many cases, the framework should take into consideration groups of individuals who may not seek help at all because of concerns about, fear of, or prior negative experiences with, police involvement - especially for those who are Black, Indigenous, and racialized. The failure to build in consent from an individual victim or target illustrates the shortcomings of this regulatory framework, which attempts to regulate disparate harms such as terrorism and incitement of violence with non-consensual distribution of intimate images.

Mandatory reporting risks the over-criminalization of individuals and puts innocent people at risk of being reported to the police. Further, as noted in Alexa Dodge's report on CyberScan, mandatory reporting to the police has not proven to be effective in addressing certain forms of online harms, such as NCDII among young people, many of which will involve victim/survivors who do not want police involvement.<sup>24</sup> These harms must be taken seriously in all cases, but providing trauma-informed, survivor-centered options, rather than mandating police involvement in all cases, is essential to providing effective remedies for survivors.

While not strictly within LEAF's mandate, we note the serious risks to the substantive equality of marginalized groups in potentially requiring the mandatory flagging and reporting of terrorist content or content that incites violence, as each risks capturing content created and promoted by marginalized groups protesting state violence, and over-policing racialized communities, particularly if algorithms are used to identify content and mandatory reporting policies are in place. The requirement that OCSPs ensure their notifications to law enforcement do not result in differential treatment on a prohibited ground<sup>25</sup> is insufficient.

### D. The Timeframe for Takedown Requirements Must Be Tailored for Different Harms

Expedient removal of harmful online content must be balanced with freedom of expression interests and aim to avoid over-removal and wrongful takedowns. For this reason, each of the five categories of "online harms" in the framework require different timelines. For sexual images shared without consent, timeliness of removal is of utmost importance for those featured in the images.<sup>26</sup> Unlike other forms of online harms identified within the framework,

<sup>&</sup>lt;sup>23</sup> Deplatforming, supra note 4 at 227.

 <sup>&</sup>lt;sup>24</sup> Alexa Dodge, "Deleting Digital Harm: A Review of Nova Scotia's CyberScan Unit" (August 2021), online (pdf):
 VAW Learning Network < <u>http://www.vawlearningnetwork.ca/docs/CyberScan-Report.pdf</u>> [Digital Harm].
 <sup>25</sup> Technical Paper, supra note 11 at 8.

<sup>&</sup>lt;sup>26</sup> Emily Laidlaw & Hilary Young, "Creating a Revenge Porn Tort for Canada" (2020) 96 SCLR (2nd) 147.

intimate images and child sexual abuse materials are much easier to identify in content removal procedures. The harms caused by their distribution are vastly increased the longer the content stays online and is available to be downloaded, viewed and shared by others. The salutary effects of swift content removal outweigh the deleterious effects to the free expression of those affected by those immediate takedowns. This balancing will not be the same for the other harms listed in the proposal. We support expedient takedown requirements for child sexual abuse material and NCDII and images, have profound impacts on the equality interests of those targeted in these images are easier to identify than other forms of harmful online content discussed in the framework, reducing the likelihood of over-removal or wrongful takedown of such images.

However, any proposed legislation, and those responsible for implementing and administering it, must remain alive to how an expedient takedown rule for NCDII could negatively impact sex workers and other people who are expressing themselves sexually online. The regulatory body must invest resources in the relevant expertise to distinguish abusive and exploitative distribution of intimate images from instances where groups or individuals are misusing complaint mechanisms to attack and silence those with non-normative sexual identities, or those who engage in consensual non-normative sexual practices.<sup>27</sup> "Deplatforming Misogyny" provides an example of such negative impacts when discussing the consequences of US Senate bill *Stop Enabling Sex Traffickers Act* (SESTA) and the House Bill *Allow States and Victims to Fight Online Sex Trafficking Act* (FOSTA), enacted in April 2018, which resulted in social media companies prohibiting and removing vast amounts of legitimate sexual expression content - including sex education materials - in order to protect themselves from liability under these statutes which were intended to prohibit exploitative content.<sup>28</sup>

#### E. Necessity of Transparency and Disaggregated Data from Platforms on All Instances of

#### TFGBV

We also support imposing an obligation for OCSPs to provide regularly scheduled reports to the Digital Safety Commissioner about their content moderation practices.<sup>29</sup> However, we urge the government to expand the OCSPs' reporting obligations by requiring them to submit disaggregated demographic data in all instances of TFGBV (such

<sup>&</sup>lt;sup>27</sup> See Ari Waldman, "Disorderly Content" (16 August 2021), online (pdf): Available at SSRN

<sup>&</sup>lt;a href="https://ssrn.com/abstract=3906001">http://dx.doi.org/10.2139/ssrn.3906001</a> [Disorderly Content].

<sup>&</sup>lt;sup>28</sup> Deplatforming, supra note 4 at 139.

<sup>&</sup>lt;sup>29</sup> Technical Paper, supra note 12 at para 14.

as NCDII and hate speech) so that researchers and civil society organizations can accurately glean how misogyny, racism, ableism, homophobia, and other forces of oppression are impacting the platforms. Currently, the framework only requires OCSPs to provide disaggregated data when the incidents of online harm are shared with law enforcement.<sup>30</sup> Content moderation transparency reporting obligations should not be tied to reports to law enforcement agencies, nor, as noted above, should OCSPs be required to report every incident of TFGBV to law enforcement.

One of the recommendations in "Deplatforming Misogyny" was to require digital platform companies to "undergo independent audits [...] and publish comprehensive annual transparency reports."<sup>31</sup> We also recommended that the transparency reports that the data in the report "should be broken down by demographics (particularly gender and race) to the extent possible, regarding the platform's internal content moderation policies and practices, and regarding the prevalence of and efforts to address TFGBV, as well as the results of those efforts."<sup>32</sup> Requiring data from platforms will be critical for academics and civil society organizations to understand OCSP's content moderation practices and gather the relevant information in order to conduct research and/or advocate for equality-centered reform.

Regulatory requirements including content moderation reporting needs to differentiate between platforms of various sizes, natures, purposes and business models. Regulations should not be so burdensome that it will prevent smaller sites or companies from complying with them or beginning at all. This consideration needs to be taken into account on all aspects that the government seeks to legislate.

F. Issues Regarding a Digital Safety Commissioner

Taking into consideration the critiques made above, we support the establishment of a government body or bodies such as the Digital Safety Commissioner and Digital Recourse Council of Canada, so long as the government revises the approach of the regulators to an equality-based one. This means that the regulator must have the objective of providing accessible and meaningful remedies to those targeted by TFGBV and actively seeking to adjust norms and behaviours around TFGBV through public education and evidence-based research.

The current framework has some positive aspects to it, including:

<sup>32</sup> *Ibid*,

<sup>&</sup>lt;sup>30</sup> *Ibid* at para 14 (h)(II).

<sup>&</sup>lt;sup>31</sup> Deplatforming, supra note 4 at p. 229 (Recommendation #10).

- Requirements for the Commissioner to engage with groups disproportionately affected by harmful online content;
- Requirements that Online Communication Service Providers (OCSP) provide reports of their content moderation practices;
- Requirements that social media companies have clear content moderation guidelines;
  - Inclusion of a formal complaints process for individuals to make complaints of noncompliance with regulations and failure to follow content moderation guidelines;
  - Administrative monetary penalties (AMP) for ongoing non-compliance;
  - Recognizing that "hatred spread online often has a disproportionate impact on women, Indigenous Peoples, members of racialized and religious minority communities and on LGBTQ2 and gender-diverse communities and persons with disabilities" and that "that OCSs are used to sexually exploit children online, and that such exploitation can have life-long consequences for victims";
  - Requirements that flagged content be addressed expeditiously (however, the current approach on timing must be reexamined depending on the content flagged);
  - Supports for platforms in reducing harmful content;
  - Engagement in partnerships, education outreach activities, and research on TFGBV;
  - Requirements that members of the commission, council and advisory body have subject matter expertise and are inclusive of marginalized communities and groups protected under the *Canadian Human Rights Act*.

The framework for these bodies could be improved by taking the following considerations into account:

- The proposed regulatory bodies should provide accessible and immediate supports for victim/survivors of TFGBV as well as more systemic responses.
- Governmental bodies that provide targets of TFBGV with direct support, administrative support, and educational campaigns have proven to be useful to those individuals impacted by TFGBV.<sup>33</sup> <u>Research has shown what is most commonly needed by</u> victim/survivors of TFGBV is immediate technical safety support such as support in getting content taken down as well as emotional support and information from people with subject matter expertise.<sup>34</sup>
- In many cases of non-consensual distribution of intimate images, what victim/survivors need is immediate support navigating social media company's content moderation

<sup>&</sup>lt;sup>33</sup> Pam Hrick, *The Potential of Centralized and Statutorily Empowered Bodies to Advance a Survivor-Centered Approach to Technology-Facilitated Violence Against Women* (Bingley, UK: Emerald Publishing, 2021) [*Centralized and Statutorily Empowered Bodies*].

<sup>&</sup>lt;sup>34</sup> Digital Harm, supra note 24,

processes and other tactics for getting content removed.<sup>35</sup> Even with statutory regulations that require timely content removal, victims/survivors will need accessible information and direct assistance in reporting and understanding reporting procedures and will need supports beyond simply getting the content taken down.

- The federal government should look to bodies such as Nova Scotia's CyberScan, New Zealand's Netsafe, Australia's eSafety Commissioner and the UK Revenge Porn Helpline as examples of government supported initiatives that provide immediate help to targets of TFGBV.<sup>36</sup> These bodies provide help lines, direct reporting mechanisms, and information that provide immediate support to those targeted by TFGBV and other forms of problematic behaviour online.
- These bodies have staff who understand social media companies' reporting systems and can provide assistance in getting content removed. Non-consensually distributed intimate images and child sexual abuse material is already prohibited by most major social media sites. When these organizations have established relationships with the major social media companies where the bulk of harms occur, they can provide more direct support than an individual can. For example, in 2018, the eSafety Commissioner of Australia was able to have 90% of the NCDII reported to them removed.<sup>37</sup>
- The proposal requires that prohibited content not be available in Canada. This is
  unclear whether the content will be deleted, as is necessary for NCDII and CSAM, rather
  than blocked for Canadian users through geolocation/IP filtering. NCDII and CSAM must
  be deleted and not be accessible to any users.
- These supports should be buttressed with regulatory requirements that social media companies remove particularly harmful forms of content in a timely manner and penalties for failing to do so. This is necessary because many social media companies will otherwise be incentivized to allow harmful forms of TFGBV to remain on their platforms if this content is lucrative or drives up user engagement.<sup>38</sup>
  - Statutory and regulatory requirements, along with government supported bodies that can provide immediate support and remove the burden from targets and place greater obligations on platforms that have to date failed to adequately address TFGBV on an individual and systemic level.

<sup>35</sup> Ibid.

<sup>&</sup>lt;sup>36</sup> Centralized and Statutorily Empowered Bodies, supra note 33.

<sup>&</sup>lt;sup>37</sup> Australian Government, "Annual Reports 2018-19: Australian Communications and Media Authority Office of the eSafety Commissioner" (2018-19), online: *ACMA* <<u>https://www.esafety.gov.au/sites/default/files/2019-</u>10/ACMA\_and\_eSafety\_annual\_reports\_2018\_19.pdf>.

<sup>&</sup>lt;sup>38</sup> Deplatforming, supra note 4 at 53-54; See also Georgia Wells, Jeff Horwitz and Deepa Seetharaman, "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show", Wall Street Journal (14 September 2021), online: <a href="https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=article\_inline">https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girlscompany-documents-show-11631620739?mod=article\_inline>.

- These organizations should provide technical and emotional support to those harmed by content that is not illegal, such as getting content removed that breaches a social media company's content moderation policies or providing emotional and technical support to those who have been targeted by TFGBV.
- These direct support mechanisms should be accessible 24 hours a day and should provide phone, email and texting options so the harms can be addressed at the time that they occur.
- It should be noted that non-normative and LGBTQ+ content is more likely to be inappropriately flagged, taken down and banned. As such, there also need to be timely mechanisms in place to challenge when this content is inappropriately flagged and made inaccessible in order for that content to be made accessible again<sup>39</sup> through an accessible and timely counter notification process.<sup>40</sup>
- Requiring victims/survivors to engage in a regulatory process that will take weeks or months is not a viable solution for people whose sexual images have been posted online. As noted by Alexa Dodge, when there are few supports and a complex system to report TFGBV, people are unlikely to engage in the very systems meant to protect them.<sup>41</sup>
- In more extreme cases where the perpetrator refuses to take down content, social media companies fail to properly implement their content moderation guidelines, or content is posted on websites that are dedicated to hosting TFGBV, such as revenge websites, additional government support is needed. In these situations, a formalized process through a digital safety commissioner or other body could be helpful to address these issues.
- In cases where the victim/survivor is interested in pursuing a criminal response, meaningful support for them should be available. It is well documented that victims of sexual violence have experienced unsupportive and discriminatory responses from some criminal justice system actors, including police officers and the courts. Any regulatory body set up to address TFGBV should work with those in the criminal justice system to ensure they do not mistreat or revictimize women and others who have been the targets of TFGBV. In all cases, the choice of whether or not to engage with the criminal justice system must remain with the victim/survivor, and not forced upon them.

<sup>&</sup>lt;sup>39</sup> Disorderly Content, supra note 27.

<sup>&</sup>lt;sup>40</sup> Sonja Solomun, Maryna Polataiko & Helen Hayes, "Platform Responsibility and Regulation in Canada: Considerations on Transparency, Legislative Charity, and Design" (2021) 34 Harv JL & Tech < <u>https://jolt.law.harvard.edu/digest/platform-responsibility-and-regulation-in-canada-considerations-on-</u> <u>transparency-legislative-clarity-and-design></u>.

<sup>41</sup> Digital Harm, supra note 24.

- Victim/survivors should be empowered to choose their own course of action and should have multiple courses of action, including formal and informal responses.<sup>42</sup> This may include flagging and removing content, engaging with law enforcement agencies when the behaviour is criminal, and/or speaking with a specialist in TFGBV who can provide emotional and technical support to manage the incident.
- The educational material produced by this body should encourage a cultural shift in attitudes toward TFGBV specifically and gender-based violence. This should be done in the school system and for the larger public.<sup>43</sup>
- Ongoing research should be conducted on TFGBV to understand trends and examine the effectiveness of government responses, including regulatory and criminal ones. This research must be informed by evidence based on the experiences of victim/survivors.<sup>44</sup>
- G. Increasing the Focus on Education and Prevention

An effective regulator of online harm must not only provide remedies to online harm that occurs, but also proactively seek to change the culture by educating the public and the decision-makers about the oppressive roots of TFGBV.<sup>45</sup> For this reason, we urge the government to identify research and education as one of the central mandates of the Commissioner to prevent future acts of TFGBV.

Currently, education only gets a cursory mention in the Technical Paper, which states the Digital Safety Commissioner will engage in "[p]artnerships, education and outreach activities, and research" to help fulfill the policy objectives of the new legislation.<sup>46</sup>

The research and education function should not be just geared towards government and academics, but to the public at large. In order to effectively serve a preventative function, the education materials should be publicly accessible in format and content.

<sup>&</sup>lt;sup>42</sup>Centralized and Statutorily Empowered Bodies, supra note 33.

<sup>43</sup> Ibid.

<sup>44</sup> Ibid.

<sup>&</sup>lt;sup>45</sup> Anastasia Powell et al., "Image-based sexual abuse: An international study of victims and perpetrators. A Summary Report" (February 2020) at 12, online (pdf): *RMIT University* 

<sup>&</sup>lt;a href="https://researchmgt.monash.edu/ws/portalfiles/portal/319918063/ImageBasedSexualAbuseReport\_170220\_W">https://researchmgt.monash.edu/ws/portalfiles/portal/319918063/ImageBasedSexualAbuseReport\_170220\_W</a> EB 2.pdf>.

<sup>&</sup>lt;sup>46</sup> Technical Paper, supra note 12 at para 35(b).

Page 18

#### H. Dangers of Algorithmic Moderation

As anticipated in the framework, algorithmic identification of harmful content will be required by larger platforms to comply with the framework's requirements. This raises serious equality concerns, as <u>algorithms have not proven to be failsafe mechanisms for identifying</u> and removing harmful content, particularly content that requires detailed analysis such as hate speech. This adds a significant risk of over-compliance and the removal of legitimate content.

Proactive algorithmic based removal of child sexual abuse material may be appropriate in most circumstances, however, in cases of NCDII algorithms will not be suited to identify the difference between legitimate images of sexual expression and those posted without consent. In the case of NCDII, content that is flagged as NCDII should be removed immediately.

Additionally, the use of algorithmic moderation poses serious substantive equality concerns. There is significant scholarship about the discriminatory impact of these systems.<sup>47</sup> In the realm of content moderation, the distributive harms stemming from the use of these algorithms will largely be experienced by gender-diverse, racialized, Indigenous and other marginalized communities.<sup>48</sup> This has already occurred in the United States in the context of hate speech; research from 2019 showed that AI models for detecting hate speech online were more likely to flag tweets from Black posters as offensive or hateful.<sup>49</sup> The reason for this is that algorithms do not produce neutral outcomes; instead, the outcomes reflect the biases of their designers and the biases contained in the data that they are constructed and trained on.<sup>50</sup>

\*\*\*\*\*

We would welcome an opportunity to discuss any of the above further.

<sup>&</sup>lt;sup>47</sup> For discussing the role of bias in data and what can be done about it, see: Solon Barocas & Andrew D. Selbst, "Big Data's Disparate Impact" (2016) 104 Cal L Rev 671

<sup>&</sup>lt;https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2477899>

<sup>&</sup>lt;sup>48</sup> Robert Gorwa, Reuben Binns & Christian Katzenbach, "Algorithmic content moderation: Technical and political challenges in the automation of platform governance" (28 February 2020), online: *Big Data & Society* <<u>https://journals.sagepub.com/doi/full/10.1177/2053951719897945</u>>.

<sup>&</sup>lt;sup>49</sup> See for example Shirin Ghaffary, "The algorithms that detect hate speech online are biased against black people" (15 August 2019) online: *Vox* <<u>https://www.vox.com/recode/2019/8/15/20806384/social-media-hate-speech-bias-black-african-american-facebook-twitter</u>>

<sup>&</sup>lt;sup>50</sup> Sandra G Mayson, "Bias in, Bias out" (2019) 128 Yale LJ 2218

<sup>&</sup>lt;https://www.yalelawjournal.org/pdf/Mayson\_p5g2tz2m.pdf>.

# Appendix: Full List of Recommendations from "Deplatforming Misogyny"

From Cynthia Khoo, "Deplatforming Misogyny" (April 2021), online (pdf): *Women's Legal Education and Action Fund* <<u>https://www.leaf.ca/publication/deplatforming-misogyny/</u>>:

#### Guiding Priorities and Recommendations for Federal Action

This report provides 14 recommendations for federal action, including legislative reform. These recommendations are based on six guiding priorities that emerged from the research and analysis conducted in this report and should govern efforts to address TFGBV in Canadian law.

These priorities are:

- recognizing a need for legal reform to address TFGBV, including through platform regulation;
- recognizing that Canadian constitutional law justifies imposing proportionate limits on
- freedom of expression in order to uphold and protect the rights to equality and freedom from discrimination, and also to give full effect to the core values underlying freedom of expression;
- guaranteeing that legal reforms that address TFGBV build in victim/survivor-centered, trauma-informed, and intersectional feminist perspectives;
- ensuring expedient, practical, and accessible remedies for those targeted by TFGBV;
- providing due process mechanisms to users who wish to contest platforms' content
- moderation decisions (whether a decision to leave up or take down content); and
- requiring transparency from platform companies regarding their content moderation policies and decisions, as well as the outcomes of such policies and decisions concerning TFGBV.

### Recommendations for Federal Action

### A. Centering Human Rights, Substantive Equality, and Intersectionality

- 1. Apply a principled human rights-based approach to platform regulation and platform liability, including giving full effect to the rights to equality and freedom from discrimination.
- 2. Ensure that legislation addressing TFGBV integrates substantive equality considerations and guards against exploitation by members of dominant social groups to silence expression by members of historically marginalized groups.

 When pursuing legislative or other means of addressing TFGBV, consult substantively with and take into account the perspectives and lived experience of victims, survivors, and those broadly impacted by TFGBV.

#### B. Legislative Reforms

- 4. Establish a centralized expert regulator for TFGBV specifically, with a dual mandate: a) to provide legal remedies and support to individuals impacted by TFGBV on digital platforms, including regulatory and enforcement powers; and b) to develop research on TFGBV and provide training and education to the public, relevant stakeholders, and professionals.
- Enact one or more versions of the current 'enabler' provision in subsections 27(2.3) and 27(2.4) of the Copyright Act, adapted to specifically address different forms of TFGBV, including 'purpose-built' platforms.
- Enact a law that allows for victims/survivors of TFGBV to obtain immediate removal of certain clearly defined kinds of content from a platform without a court order, such as NCDII.
- 7. Ensure that legislation to address TFGBV focuses solely on TFGBV (including intersectional considerations)—do not dilute, compromise, or jeopardize the constitutionality of such legislation by 'bundling' TFGBV with other issues that the government may wish to also address through platform regulation.

#### C. Legal Obligations for Platform Companies

- Require platform companies to provide to users and non-users clearly visible, easily accessible, plain-language complaint and abuse reporting mechanisms to expediently address and remedy instances of TFGBV.
- 9. For 'purpose-built', 'enabling', or otherwise TFGBV-dedicated platforms, and where a clearly delineated threshold of harm is met, provide that an order to remove specific content on one platform will automatically apply to any of that platform's parent, subsidiary, or sibling platform companies where the same content also appears.
- 10. Require platform companies to undergo independent audits (which could be conducted by the new TFGBV agency) and publish comprehensive annual transparency reports.
- When determining legal obligations for digital platforms, account for the fact that platforms vary dramatically in size, nature, purpose, business model (including nonprofit), extent of intermediary role, and user base.

#### D. Research, Education, and Training

- 12. Fund, make widely available, and mandate (where appropriate) education resources and training programs in TFGBV, which include information on how to support those who are subjected to TFGBV.
- 13. Fund frontline support workers and community-based organizations working to end, and supporting victims/survivors of, gender-based violence, abuse, and harassment, specifically to enhance their internal expertise, resources, and capacity to support those impacted by TFGBV (which often accompanies gender-based violence and abuse).
- 14. Fund further empirical, interdisciplinary, and law and policy research by TFGBV scholars, other TFGBV experts, and community-based organizations on TFGBV and the impacts of emerging technologies on those subjected to TFGBV.

Southerstein construction of the second system o

Re: The Government's approach to address harmful content online Submitted by: Rose A. Dyson Ed.D. President: Canadians Concerned About Violence In Entertainment Vice President: World Federalist Movement of Canada: Toronto Branch Author: *MIND ABUSE Media Violence And Its Threat To Democracy* (2021) email: <u>rose,dyson@alumni.utoronto.ca</u> or <u>rdyson@oise.utoronto.ca</u> Phone: 416-961-0853 or 647-382-4773

#### **Dear Committee Members**

Thank you for the opportunity to participate in this discussion on meaningful action to combat hate speech and other kinds of harmful content online. Public concern about harmful media content has now been with us for several decades and the need to address the problem has gotten increasingly urgent. The five categories identified as hate speech and other kinds of harmful content online, including child sexual exploitation, terrorist activity, content that incites violence, and the non-consensual sharing of intimate images have skyrocketed as communications technologies have evolved.

As far back as 1975 Judy La Marsh, a lawyer, journalist and former member for the Liberal Government of Canada was appointed by the Government of Ontario to chair the Royal Commission on Violence in the Communications Industry. It was empowered to study the effects on society of increasing violence in the media of the day and make appropriate recommendations on measures to be taken by different levels of government, by industry and the public at large. Most of the 80 plus recommendations have never been implemented. Some have been repeated in subsequent studies but still not implemented.

In my doctoral thesis, completed at OISE/UT in 1995, I reviewed the research findings conducted by the La Marsh Commission and other studies done up until that time, subsequent recommendations and evidence or lack thereof regarding implementation. Two books on the subject followed. The first published in 2000 and the second earlier this year. A complimentary copy of either one is available upon request. The latest is titled, *MIND ABUSE Media Violence And Its Threat To Democracy*, (2021) Over the past 30 years I have watched the problems mushroom with increasing evidence of commercial reliance on themes of sex and violence in media production. In addition we have had fading boundaries between different forms of media. These include news, fiction, advertisements and educational programming, leading to catch phases such as edutainment and infotainment.

Digital technologies and the internet have magnified the problems with policy makers loath to take on the challenge of much needed and overdue regulation, frequently to avoid accusations of censorship. Inadequate distinctions between individual freedom of expression and corporate freedom of enterprise have persisted. Periodic studies funded by industry are released into the public domain countering evidence of harmful effects thus ensuring no interruptions to business as usual. For decades the cultural industries have been given carte blanche to determine what we see, hear and read.

In 1996, along with 250 other scholars and media activists representing over 88 organizations from around the world, I helped the late George Gerbner, an internationally renowned media scholar, launch the Cultural Environment Movement at Webster University in St. Louis. That Convention was preceded by the International Summit on Broadcast Standards attended by Keith Spicer, then chair of the CRTC and other Canadians representing business and non-profits. In his work, Gerbner frequently referred to violence creep in popular culture and other forms of media, including news and advertisements, as the hidden curriculum for a Mean World Syndrome.

My colleague, retired U.S. Lte. Col. David Grossman, a psychologist and Military Expert, has written 5 books on the subject of violent first person shooter video games and the dangers of indiscriminately marketing these games to the youngest most vulnerable people on the planet. In his latest book, *Assassination Generation Aggression, Video Games and the Psychology of Killing* (2016) he provides chilling detail on how these have led to mass murders and fueled terrorism. Grossman reveals how violent video games have ushered in a new era of mass homicides worldwide. The trends have led to what he calls Acquired Violence Immune Deficiency Syndrome.

The kind of online hate and extremism that led to the January 29, 2017 mass murders at the Centre culturel islamique de Quebec, and on March 15, 2019, in Christchurch, New Zealand, is inherent in the thematic content of numerous video games played by the killers. In both cases news coverage identified evidence of heavy diets of first person shooter video game playing on the part of these perpetrators. This is a pattern that is described over and over again by other researchers among them, Mark Bourrie, author of *Martyrdom, Murder and the Lure of Isis*, and Megan Condis, author of *Gaming Masculinity, Trolls, Fake Geeks, and the Gendered Battle for Online Culture*.

What must be recognized is that the Government's focus on regulating social media and combating harmful content online cannot be confined to "speech only". Violent forms of fictional entertainment such as video games depict storylines that glorify violence, hatred, anti semitism and sexual exploitation. It would be duplicitous and of marginal value to address the problems involving work place harassment, misogyny and other excesses on the internet but to leave such content in popular culture unaddressed and unregulated. Countless studies over the years have demonstrated that these fictional depictions lead to learned behaviours based on psychological conditioning that result in distorted value systems, a tendency to resort to violence as a conflict resolution strategy, addiction and feelings of victimization, among other harmful effects.

It has also been demonstrated that violent, first person shooter video games provide fertile soil for sowing the seeds of resentment among young vulnerable white males. An "us versus them" mentality is encouraged, helped along by social media algorithms that capitalize on our genetic tendencies to respond quickly to negative themes. It has also been reported that white supremacist groups watch the latest releases of video games that are most amenable to their purposes of recruitment. Some have taken to producing their own.

The work being done by technology experts like the Institute of Electric and Electronic Engineers (IEEE) on a roadmap for 5G and global integration to facilitate the more efficient use of energy must also focus on the nature of energy use. Spokesmen on behalf of the Institute now stress that more efficient use of what is rapidly becoming unsustainable energy demand on the internet is essential and required to reduce both collective and individual carbon footprints. But, clearly, emphasis on discretionary use is also required. Assuming we are put on a war time footing, as advocated by Seth Klein in his book, *A Good War: Mobilizing Canada For The Climate Emergency* (2021), rationing of internet use will have to be adopted. In December, 2020, Nicholas Kristoff wrote in the *New Yor k Times* that Pornhub, owned by Mindgeek in Montreal, was the third most visited and influential website on the Internet. It is inconceivable, in a world focused on sustainability and transitioning to clean energy that, on the Internet, harmful excesses are overlooked and excused as essential components to be protected under the umbrella of civil liberties. Surely the expertise in electronic engineering should not be misdirected in the race against time to ensure internet use that fosters social harm.

There are also concerns expressed by health advocates, such as Devra Davis, author of *DISCONNECT The Truth About Cell Phones, What the Industry Has Done To Hide It and How To Protect Your Family* (2010), about harmful radiation from digital devices that can cause cancer. In this context it behooves the government to take note of the recent United States Court of Appeals for the District of Columbia Circuit judgement in favour of environmental health groups. It found the Federal Communications Commission (FCC) in violation of the Administrative Procedures Act for not responding to comments on environmental harm. In short, the FCC failed to respond to record evidence that exposure to low level radiation from digital devices may cause negative health effects

#### Re: Strategy to combat hate speech and other harms:

We endorse the move to amend the Canadian Human Rights Act to enable the relevant Commission and Tribunal to review and adjudicate hate speech complaints.

- \* But, over reliance on industry, itself, to monitor social media content, has proven in the past to be an exercise in futility. One minor exception involves the Canadian Broadcast Standards Council which was set up in 1993 by the Canadian Association of Broadcasters to respond to complaints of inappropriate content on radio or television programming. This Council could be expanded or duplicated to monitor online content. However, the Council has always been reactive rather than proactive with no oversight for industry excesses unless complaints arise from the public at large. That needs to change. Allowing the fox to guard the henhouse with no government oversight has never worked.
- \* Second, definitions of obscenity and sections on child pornography need to be updated and expanded. Research conducted in the latter part of the last century, demonstrates how all pornography can be addictive. In addition it involves social learning theories that lead to themes of aggression and dominance. These tendencies can trickle down to the most vulnerable targets of exploitation which are children. Before the bill on child pornography, making possession, production and distribution a crime was passed in 1993,

considerable attention was paid by the Government's Standing Committee on Culture and Communications set up at that time. It came out with a number of additional recommendations that were never implemented. One of them was to determine the criminal legislative measures needed to include extremely violent forms of entertainment in the Criminal Code in ways that would conform with the *Charter of Rights and Freedoms*. See *MIND ABUSE Media Violence In An Information Age* (Dyson, 2000).

- \* The objective to authorize the Government to include or exclude categories of online communication service providers from the application of the legislation within certain parameters is important but there must be complete transparency on how this will be done and who will provide expert advice on these parameters. Advice must be sought from health providers and other researchers not beholden to industrial interests.
- \* Film and video game monitoring of media content for entertainment purposes is now undertaken by provincial classification boards. A national system would be much more efficient. While great care has been taken over the years to ensure gender and racial diversity on most boards the overall tendency has been for them to bend to the will of industry. Criteria on what is age appropriate should involve input from child development experts. This has yet to happen. Indeed, the prevailing standard for most classification boards throughout the developed world has been set by the industry funded and operated, Hollywood based Motion Picture Association of America. That needs to change.

\* Legislation should be passed on a national level to ban advertising to children 13 years and under. Such legislation has been in effect in Quebec for over 25 years. From time to time, bills for implementation have been introduced in Canada at the national and provincial levels of government, boards of health and in 2016 even an editorial in *Globe and Mail*, called for one. Most developed countries have already adopted this kind of legislation, citing various concerns, among them, protecting children from harmful sexual exploitation, violent content, all advertising, the marketing of junk food known to cause physical health problems such as obesity and heart disease and the dangers of exposure to low level radiation from the internet.

The Committee must not allow itself to be intimidated by industry push back. On January 14, 2019, it was reported in *The Globe and Mail*, that a proposal from Health Canada to amend the Food and Drug Act by restricting food and beverage marketing to children had hit a familiar snag: industry protests that such regulation was "unrealistic", "punitive" and "commercially catastrophic". The huge jump in commercial exploitation of children in recent decades is nothing short of tragic. According to the Harvard Medical School founded, Boston based, Campaign for a Commercial-free Childhood, over \$17 billion was spent by the industry in 2006 in the U.S. alone to market products to children, a staggering increase over \$100 million spent in 1983. Over \$500 billion in purchases annually by that time was estimated to be influenced by children under the age of 12 years. These trends are clearly at odds with efforts focused on reducing consumer driven

Southand Construction for the contract of t

habits to facilitate future sustainability.

\* A very popular solution for dealing with harmful media has always been better vigilance from parents, along with media and digital literacy taught in schools by teachers. Although it is obvious that the problem is too big and pervasive and that better cultural policy is also urgently needed, there is room for improvement in the provision of reliable, fact based educational resources. Over the years there has been increasing evidence of subtle, industry friendly resources creeping into school curriculums on the subject. In 1975, the La Marsh Commission recommended that an Advisory Board of educators, health professionals and parents be established at the Ontario Institute for Studies in Education at the University of Toronto for the provision of public education. I reiterated the recommendation in my doctoral theses completed at the Institute in 1995, and again in my two subsequent books on media violence. Nevertheless, it has yet to be established. Better government funding and support is also needed for NGOs, such as Internetsense First, founded by Charlene Doak Gebauer, which now provide urgently needed help to parents and teachers on digital supervision.

\* Funding that is independent of industry donors, should be mandatory to ensure accuracy in monitor media violence and other harmful trends on the internet. Important models were established at the Annenberg School of Communication, University of Pennsylvania and Temple University in Philadelphia, by the late George Gerbner. The Cultural Indicators Model, later expanded into the "Fairness" Indicators Model and used by Paquette and de Guise at Laval University in Quebec City in their study Index of Violence in Canadian, Television done in 1994, is one example.

- \* An Act respecting the mandatory reporting of Internet child pornography by persons who provide an internet service is needed. But it is not clear how this would interface with the Mandatory Reporting Act.
- \* New legislation requiring regulated entities to monitor harmful content through the use of automated systems based on algorithms would be a useful way to use the new technology for prosocial purposes, given the widespread evidence of how algorithms are currently employed solely for the purposes of financial gain and fostering errant behaviour.
- \* Now, within universities across Canada and beyond, there is growing emphasis of courses offered in esport involving first-person shooter video games. This is counter productive to advocacy from experts calling for critical thinking skills, media and digital literacy and studies which point to harmful effects. There has also been ample evidence reported in *The Globe and Mail*, of generous subsidies given to video game industries such as *Ubisoft* without any regard for the nature or content involved in the productions. Tax breaks and subsidies for harmful video game production and distribution is no more justifiable than breaks for fossil fuel industries in a time of climate crisis. As pointed out by *Globe and Mail* business reporter Scott Barlow, this poses a moral dilemna (Barlow, October 14, 2017). Furthermore, these must also not be excused or spun by industry pundits as

"funding for electronic arts".

- \* It is stated that regulated entities would be required to notify law enforcement in instances where there are reasonable grounds to suspect imminent risk of serious harm to any person or property from potentially illegal content falling within the five categories of harmful - terrorist content; that which incites violence; hate speech; non-consensual sharing of intimate images; and child sexual exploitation. But it is stated that there would be no obligation to report such content to law enforcement or CSIS. Why not?
- \* And why would the threshold for such reporting of potentially terrorist and violent extremist content be lower than that for potentially criminal hate speech?
- \* The proposed legislation for a new Digital Safety Commission of Canada to support three bodies that would operationalize, oversee and enforce the new regime sounds promising. But who exactly would sit on the final stage of recourse on the Recourse Council? Diverse expertise and membership that is reflective of the Canadian population is essential to avoid having such a Council stacked with former or retired officials sympathetic to the concerns of industry. This would necessitate expertise from the health and social sciences. Transparency in public reporting obligations would also be required.
- \* An Advisory Board that would provide both the Commissioner and the Recourse Council with expert advice must include more than expertise on emerging industry trends, technologies and content-moderation standards. Who would be expected to provide information on "content-moderation standards". Like the recommended advisory group for parents and teachers, with funding independent of industry sources and the Recourse Council, such a Board should include social science expertise and input from both physical and mental health experts. Having the Digital Safety Commissioner of Canada mandated to lead and participate in research and programming, convene and collaborate with relevant stakeholders and support regulated entities in reducing the five forms of harmful content will only work if input is not confined to industry related interests. Again, the composition of the Advisory Board must include, along with all the other stakeholders itemized, health expertise.

#### **Re: Compliance and enforcement**

\* The powers of the Commissioner are necessary and sound reasonable.

# Re: Modifying Canada's existing legal framework including the Canadian Security and Intelligence Act (CSIS)

\* Centralizing mandatory reporting of online child pornography offences through the RCMP's National Exploitation Crime Centre to ensure stronger requirements for internet service providers for reporting excesses would help but continuing vigilance to ensure that is happening must be provided. Not requiring judicial authorization in reports to law enforcement is necessary to expedite police response in cases where an offence is clearly

evident. The same criteria should be applied to CSIS to ensure more timely access to relevant information that could help mitigate the threat of online violence extremism. For this process to take 4-6 months, as it does now, seriously diminishes their capacity to be effective.

Again, thank you for the opportunity to participate in this timely discussion. If provision is made for appearance via zoom before the committee to submit a statement I would appreciate the opportunity.

#### **References:**

Barlow, S. (2017b, October 24) Getting hooked on gaming stocks. The Globe and Mail. P.B6.

Barlow, S. (2017a, October 14) As investing theme video games score big. *The Globe and Mail*. P.B3.

Bourrie, M. (2016). The Killing Game: Martyrdom, Murder and the Lure of ISIS. Toronto, ON: Harper Collins Canada

Condis, M. (2018) Gaming Masculinity: Trolls, Geeks and the Gendered Battle for Online Culture. Iowa City, IA: University of Iowa Press.

Davis, D. (2010). The TRUTH About Cell Phone RADIATION: What the INDUSTRY has Done to Hide It, and How to PROTECT Your FAMILY. New York: Dutton.

Doak-Gebauer, C. (2019) THE INTERNET: ARE CHILDREN IN CHARGE? Tellwell, Canada.

Dyson, R. A. (2000). *MIND ABUSE: Media Violence in an Information Age*. Montreal: Black Rose Books.

Dyson, R.A. (2021). *MIND ABUSE: Media Violence and its Threat to Democracy*. Montreal: Black Rose Books. UT Press, AMAZON

Grossman, D. (2016). ASSASSINATION GENERATION: Video Games, Aggression and the Psychology of Killing. Boston, MA, Little, Brown & Company.

Klein, Seth. (2021). A Good WAR: Mobilizing Canada For The Climate Emergency. Amazon: U.S.

United States Court of Appeals for the District of Columbia. EHT Victorious in Federal Court Case Against FCC on Wireless Radiation Limits. August 14, 2021.

PhotParS0 - odb265465 ccccatter 33, - or 2<sub>10</sub> - 2<sub>10</sub><sup>2</sup> - of attraction 250, open/attraction open open (2) is - traction (2) - 0,052

# Felicia Mazzarello

		s.19(1)	
From:	Ash Hulewicz	5.19(1)	
Sent:	August 19, 2021 2:12 AM		
To:	ICN / DCI (PCH)		
Subject:	Having My Say		
Categories:	Cathy		

To whomever is reading this from the Digital Citizen Initiative,

I am writing to submit my thoughts on the proposed approach to address harmful content online. A few concerns that I want to address under the following sections:

- 1. Issues with Definitions
  - 1. Private Communication on Public Platforms
  - 2. The Assumption of Public Communication
- 2. Technological Lag
  - 1. The Algorithm
  - 2. The Alternative to Al
  - 3. Chilling Effect
- 3. The "Black Market" Problem
- 4. Public Access

#### **Definitions - Public and Private Communication**

1. Private Communication on Public Platforms.

The distinction between public and private platforms online are arbitrary.

"Online Communications Services" and Private Communications Services are distinguished as separate as per their use. Though several examples of OCS are given, few are given for PCS. Though PSCs are excluded, and should be entirely private communication platforms, OSC websites do not fall within single use. Sites that would be considered OSC, such as Facebook and Instagram contain features that allow for:

a. Private messaging, and

b. Private groups.

On a., will Facebook messenger for example, be subject to the rules of OSCs because it is hosted through a public communication platform?

On b. What about "private" groups, or groups that require invite? These groups can be as small as a few people, and as large as several thousands. The way that these groups work on Facebook is through the subject "public" posting mechanism that the rest of the site uses, though access to view it is restricted to the group.

Email, as a Private Communication Service, conversely, does not happen on a one to one basis either. Users can sign up for email newsletters and have massive email group discussions. I am sending this email to a single other email, though how many people are able to access this? If it's a government email (I assume it is, given I accessed this email from a. Government site and the webaddress is <u>Canada.ca</u>), it may be likely that more than one *person* read my submissions. As part of a *public commentary initiative*, it may be documented and archived along with the other emails, *technically accessible* by an unknown number of people within the government.

The question is, at what point is a communication service **public or private?** If the issue is number of people the information could access (a magnitude metric) : emails can be sent to thousands of people, and Facebook posts can be accessed by as few as a user and a single friend. This is an arbitrary distinction.

#### 2. The Assumption of Public Communication

On nearly all social media platforms, users have the ability to restrict public access to their content for privacy.

Facebook allows personalized accounts to be fully private, or elements of their profile to be public, for friends only, for specific chosen groups of 'friends', or for the users eyes only.

Instagram allows for profiles to be public or private as well, and though the name of an account can be found, any of the published content can be private. Even for ones' "story", which is a temporary post on the platform, users can pick and choose who can see it, including smaller private groups of friends.

Youtube lets users private, or archive video content produced as well as playlists. Or, they could broadcast their content and playlists to the world.

We assume that just because anyone could *technically* access posts online, that they do. Even if a YouTube video is made public, *does the entirety of the user base on YouTube see it?* No, they do not. When you make a Facebook post with a public setting, *will a huge number of Facebook users see your post?* Not likely.

The people who are likely to access it are people within your online social circle or subscribers, where the algorithm prioritizes you to them because they have a historical record of interacting with your content. The potential additional viewers you may receive likely access your content because it hits similar keywords, hashtags, or interests, that have been expressed by that individual. We largely live in digital echo chambers, and algorithms are the intellectual private property of these companies. We don't know specifically how they work, but we see the consequences of them and can infer from there.

Seatherstell - construction in a child effect on Pacific Sector and construction incompared and an experiment of the Pacific Sector and Pacific Sector and Sector Sector and Sec

Just because people can *technically* be subjected to your content does not mean that they do. Considering how much of the digital world is a second life- I'd like to compare this situation to a public setting.

A cafe is a public space. You could have a private conversation in a public place with an old friend. Other patrons of the cafe sitting near you are *technically able to hear what you are saying*. We assume that if they did overhear your friend, that they would be eavesdropping. Your friend may get into a passionate rant about a controversial subject important to them. Maybe it's about terrorism, maybe it's about intersectional feminist discourse, maybe it's about genocide. People do talk about these things. People should talk about these things. We value independent thought in society. Now, the patrons overhear some parts of the rant. It's bits and pieces. But they don't know your friend. They don't know what's a quote, what's a joke, what's a reference, or whether to take your friend in good faith for an out of context discussion on a complete stranger. Realistically, what should the **punishment** for your friend be for *publicly subjecting others to potential hate speech*?

a. None! We assume that though you were in a public place, that your discussion with your friend was private. Other patrons may have been a bit uncomfortable and confused, but they can decide to stop listening, move, or assess that the conversation people are privately having is low impact and has very serious tangible harm.

b. Your friend should be removed within the restaurant nearly immediately. The cafe is relatively short staffed, and they do not have enough time to weigh into this conflict and try to resolve the conflict or assess who is at fault, why, or what damage has been done. If your friend isn't removed nearly immediately, the cafe should face severe financial penalties.

To my understanding, the draft proposes option b as the correct one.

Why would we assume that **de facto** private online comments and posts are public? We don't assume private conversations are public speech, even if other bystanders could *technically* hear them.

2. Technological Lag

#### 1. The "Algorithm"

The primary mechanism used in this policy to censor content is to rely on the private intellectual property of these tech companies in question: the algorithm. As I previously established, no users know what the algorithm looks like, we just see how it operates. Even if the Canadian government could access the algorithm, it is a guided AI with an unimaginably large database of site data. Would this be useful to access for the government, and does the government have the technological literacy and funding to engage with the product created by some of the most accomplished coders in the world? I'm not sure we do.

If the Canadian government is going to rely on an algorithm to play referee on acceptable speech, what constitutes inciting violence, or what constitutes "terrorism"- it should be a great algorithm, right?

Despite the multibillion dollar assets and 'cutting edge' technology, AI data screening is still in it's infancy.

I should disclose that I am not a coder, nor an employee at any tech-related company. I am a young adult, grew up in the country of Canada and multiple communities on the internet. It still plays a highly time consuming role in my life-particularly with the pandemic. I am speaking to what I can assess as somebody who *has used these sites since they were created on a daily basis* and an interest in how the spaces I use are regulated.

#### a. Detection

Detecting what constitutes a violation of these guidelines mandated by the government is going to be impossible for the foreseeable future for 2 reasons:

First, it is still incredibly unclear what these guidelines will look like. Depending on the makeup of this commission, we are expanding what kind of content is harmful to far beyond our current Hate Speech Laws under the Criminal Code.

This is uncharted territory in a lot of ways, and the discretion of these members is incredibly high. Too high even, given that this is akin to moral policing. There are endless public debates academics *right now* about whether online speech and communities are necessarily different than ones in real life. Hate groups existed before the internet, and they still exist in person and online. Identifying what kind of content is *actually harmful* is incredibly unclear in the **online context**.

Should Incel communities on reddit be censored, because we worry they could become the next Elliot Rogers?

When a news story is shared on a Facebook group of a few thousand members about ISIS current geopolitical status and an exhausted college activist makes an ironic joke about joining the cause among friends, are they supporting terrorism?

Should a consensual video of an amateur couple on pornhub get taken down because one parter has a short, slender figure that could be assessed by some as 'teenaged' or 'childlike' despite being an adult?

Context is difficult enough as people with critical thinking and the ability to assess intention. We struggle to do this online, over text and email where jokes, irony and humour is often lost in translation of the digital space. Heck, we even have difficulty in person always discerning the intention behind a comment and whether it's sincerely held, intended to hurt, coming from a place of ignorance, or an 'ironic joke'.

How could we trust an AI to effectively do this?

What does AI on these sites look likeright now?Let's look at Youtube as my favourite case study: the algorithm for in-video screening is used in 3 different ways that I am aware of, and often fails.

a. Advertisment- for monetized channels, the algorithm is used to identify 'natural breaks' where an advertisement could be placed, similar to TV breaks. Advertisements are often offered mid-sentence, at seemingly random points in YouTube videos in practice. The AI has a difficult time distinguishing music and sound effects from a persons voice, and thus interrupts conversations had in video- which are *not* natural breaks. Imagine this AI screening anything beyond noise, like abstractions of symbols. Hah!

b. Closed Captioning and Subtitles: most youtubers do not write out their scripts, conversations, or sound effects for audiences who wish to use closed captioning. Youtube's voice detecting AI will generate ones on-the-spot for you. As a person with a strong preference for subtitles whenever possible, I avoid this tool. The accuracy rate of this less than 10% in the cases where the YouTuber has an accent, and at it's best I've seen ~50%. If

Youtube's voice detecting AI cannot detect what people are saying, and 1000+ hours of content are published hourly, then how do you expect them to identify when potentially harmful language is used, and whether it should actually be dangerous or not.

C. Violent Themes and Language- Youtube has been doing this for \*ages\*. Before the government of Canada took interest, advertiser ads were sold in bundles to Youtube. Youtube would then randomly generate the allotted number of ads across videos on their platform. These ads are not tailored to the kind of content that the viewer tends to engage with, they're random. This was a hot issue when Youtube ads were introduced (when Google bought Youtube), because brands were concerned about having their product associated with videos that included politically problematic or contentious content. Despite some successful Youtube accounts having monetized status after reaching a certain audience threshold, specific videos of theirs can be demonetized if the Youtube AI detects a hidden list of controversial and non-advertiser-friendly content\*. Youtube's response to this controversy was to create this AI and demonetize this content, despite the fact that many major youtube channels rely on monetization for their income. Being demonetized for a video that could have taken 10s to 100s of man-hours can result in a 0 pay despite millions of views because it violated those guidelines. Those guidelines are not made accessible or public to youtube creators. Youtube creators have learnt through trial and error, and as a community, what is *probably* a violation and *what is not*.

\*Copyright strikes can also result in demonetization.

Youtubers know this. They can outsmart the AI. They use codewords, euphemisms, change the pronunciation fo the word, or censor part of the word, but continue to discuss content that they *know* would otherwise be flagged. I find this incredibly sympathetic, as many online figures want to engage in discussions about sensitive topics like terrorism, hate speech, and violence. They do so to protect and warn users of predatory behaviour on the platform. They do this to discuss other internet communities. They do this to talk about the world that they live in. Some of this speech I may agree with, others I most certainly do not. But we should defend people's ability to have these conversations without getting flagged, demonetized, or in the case of the policy proposed by the Liberal party- censored entirely.

For other OSCs how do they fare? With the goal of trying to be as concise as possible I won't go into as much depth for these.

Is it feasible for Pornhub, a free pornography service with very little advertising revenue to develop video AI and flagging detection systems (costlier than Youtube, because it's visual video detection), to identify the differences between adult/child, consensual/ criminal assult/ roleplay at assault, amateur porn/ revenge porn/ or modified video revenge porn.

Is it feasible for Facebook's algorithm to assess what is productive conversations, activism, or ironic humour from calls to incite violence? I think every leftist I know has threatened to "eat the rich" or far worse on these platforms. I don't think *that* is a credible threat to incite violence, though a boomer MP with poor meme literacy may disagree with me.

So then, I am highly skeptical. Are current AI models reliable at policing content? I strongly doubt it.

#### b. An Alternative to AI?

What is the alternative, relying on human employees to respond to screened reports? Well, yes. Most of these sites relied on/ rely on some amount of human screening to deal with sensitive content. This is less common now, as OSCs have grown in magnitude, and the quantity produced is too much for the comparative cost of labour.

3 problems with this model:

1. Former employees of these social media sites who worked on reported content have cited emotional fatigue, depression, and even severe PTSD. Imagine what these employees experience on a daily basis: sitting in front of a computer for 8 hours, watching nothing but visceral animal cruelty, child pomography, physical abuse, and hate speech. These employees, despite knowing that they will see violent content, cannot really consent to experience what they do. Burnout in this industry is high, for good reason. Compensation is not worth the mental anguish incurred in experiencing waves of this content, and knowing there is often nothing that they can do beyond removing the content. It is unclear which jurisdiction this violence takes place in because it is online. This content could be reuploaded and shared on other pages, and often does. This is ideally not something we should subject people to, *unless there is a serious credible threat*. And if it is, this is why we have law enforcement. Concerned friends, family, and members of a community can likely flag concerning behaviours they see from individuals who pose a risk.

Note that this policy would require social media companies to take action on removing harmful/ flagged content, and so Canadian Law Enforcement would not necessary be the ones subjecting themselves to the content.

- 2. Additionally, I already established that most people will likely never see this content because privacy settings and the algorithm both work to prohibit users from the vast majority of content out there, particularly flagged content. Why subject anybody to violent speech unless they consent to see it?
- 3. Remember my coffee shop analogy? Even if the report staff make low wages, this is an incredibly expensive endeavor. 24 hours to review and remove a report is not a lot of time. With limited time, resources, and other reports to respond to- it's not fair to assume that a human will do a better job of weighing in on how harmful a post is- the context is still likely lost.

So regardless of whether a human or an algorithm respond to content, flagged or not- we have the context problem.

#### Chilling Effect

I am the member of an 'private' online Facebook group wherein over a thousand Millenial and GenZ leftists from the Vancouver area post content that they find 'funny'. This content ranges from: internet famous 'lolcows' (people whose online presence and behaviours are milked/cow for laughs/lols), sharing image macros we agree with or disagree with. I, personally, will often repost misogynistic image macros that I find 'cringey'. I disagree with their premise and I find the representation of their hateful worldview hilarious for how simply ugly the graphic design is and how pathetic the messaging often is. I often do not provide context or commentary for my posts. I assume that members of the group assume that I post this content *because* I disagree with it, not because I agree with it. Though members of the community will provide support for my ugly political trophy with engagement. This engagement often looks like ironically seeming to agree with or applaud the bravery of such language by engaging with, what from an outside perspective could look like hatespeech. One post I had shared was a macroimage wherein a young man, wearing an American flag t-shirt, with a confederate flag backdrop, menacingly held up a katana to the camera. It something to the effect of : "I cannot be a gentleman because Feminism stabbed Chivalry in the Heart" with a bold, ugly font. As a self-identifying feminist, I found this image so striking in how ineffective it's messaging is at warning society on the 'harms of feminism'. As if to decipher the meaning of the text and explain what attitude was represented, all I had commented was "I hate women". This is what the image says behind it's edgy and bizarre presentation.

Within a few hours my post was flagged for hate speech, fully removed, and I received an account warning. I'm not upset, per se, but I am baffled. I would be surprised if my comment was flagged, given the general discourse of the page includes a lot of the same content and language that I had posted.

Why am I talking about this? This is a very low impact use of social media, and I didn't receive any severe consequences beyond a stupid post getting censored.

Online media is a space to do a lot of things. It can be a place to share thoughts, have (more or less) insightful conversations about an unlimited number of topics, it can be a way to stay informed, it can be a means to educate, and it can be a place to create public awareness and attention for social movements and rally public support.

It was the space of social media and OSC where hard conversations were had about policing and racism during the rise of BLM, with videos of police brutality, protests in Ferguson and later around the US, shared internationally.

Twitter was the space wherein Arab Spring protestors from so many authoritarian countries organized, protested, and broadcast their movement to the world.

Yes, I realize that not everybody engages with social media in this way, and prefer to just share videos of their pets, or pictures from their recent holiday to relatives and friends. But for some, it's how they connect with the world.

It can be a safe space for queer kids to explore their gender and sexuality when they are not ready/ not safe to do so at home or at school.

It can be a space where Chinese citizens, using VPNs, can connect to social media platforms and use the internet freely- whether it be to share information about their government, criticize it, or simply engage in a vast online space without oversight.

These communities are full of people. People use humor, share information, and talk about their experiences. In activist spaces, these experiences can be traumatic and refer to sensitive comment. It requires discussing problematic language/ hate speech/terrorism/ what threats of violence look like, in order to address them as a societal ill. People do this to find support, comfort, catharsis, agency over their experiences, or simply educate themselves. They may use humor, they may not use the 'right language'.

Suppose the genre of YouTube videos that aim to platform the #metoo movement, and discuss sexual violence. Did you know that survivors who share their story and use words like 'rape', 'sexual abuse', and 'pedophilia' get flagged by the algorithm?

On the context problem, you have either overworked labourers or an underdeveloped AI screening this content. In status quo, it just gets demonetized. It may get deprioritized. It may be age restricted. If Youtube were required to assess the sensitivity of a video under these conditions, with the fear of a 50 million or 5% of annual earnings penalty- the probability that they will overcorrect for the grey area of context is *very high*. Better safe, than a high fine. The potential decision of a Canadian tribunal that, with the context and review, can assess the 'danger' of the post is an unknown to YouTube. The discretion of the member is unknown. "If we are to operate in Canada.... better safe, than sorry."

I worry that this law would simply censor activism and communities that serve as safespaces. This hurts vulnerable people most. The Liberal government can cite that minorities experience more violence online (*surprise, they do in real life, too*)- but enacting a policy that could censor and sever access to these communities would hurt those same people the most.

4. The "Black Market" of Online Communities.

How many OSCs can Canada regulate and pursue financial penalties from? All of them?

Major social media companies like Facebook appeal to a large market share of the international community.

Calls for Facebook to improve its screening to avoid platforming Burmese pro-genocide propaganda succeeded in getting any Burmese literate moderators to work for the company and flag that content.

Calls for Facebook to deal with its "fake news" problem after the *Cambridge Analytica* scandal, resulted in both stock values tanking and action from the American government itself. This forced the Facebook to screen fake news, providing a warning to readers and access to articles debunking or questioning the efficacy of content.

I may regret the use of the word "forced", because this sounds like Facebook was necessarily unwilling to take action without consequence. The best way to get a company to change any undesirable behaviours is clear regulation. What is the problem? Is the problem worth solving? How should they solve the problem? Do the harms of the proposed solution outweigh the benefits?

Say this policy were successful in holding all the major OSC companies accountable for their vast user base.

If I were a user of a platform whose content was frequently censored within a short time span for trying to engage in activism, tell a joke, or engage in discourse-1 would be upset. OSCs are no longer places that I can use to talk about X or Y *at all*. 1 would look for alternative online spaces that did not tightly restrict what I could say or do.

I find another great lesson comes from the Incel community. Users who violate the Incel subreddit community's self-enforced self-policing rules for conduct can be censored and eventually removed. Whether they post content that rejects the incel ideology, is too 'extreme' for the incel ideology, or even irrelevant to the incel ideology will get removed. This community policing is relatively effective for fairly large online community spaces, all moderated by volunteers of the subreddit. But what happens to the self-identifying incels who are too 'extreme'?

They go somewhere else.

They go to a space that actively encourages a lack of limitation on speech and content. They go to 4 chan, they go to 8 chan, they go to online communities that resemble cesspools of the internets' edgiest and most rejected members. They are also entertainment grounds for those that wish to view the kinds of embarrassing, depraved, hateful, or just downright idiotic content that gets flagged and deemed actively harmful by other sites. 4chan and 8chan are infamous online for being spaces of online radicalization and predation. This is not to say that all 4chan content is disturbing, depraved, and disgusting. A lot of it can be lightly humorous and the posting aesthetic works really well for memes. But the *appeal* of 4chan and 8chan is the prevailing idea that 'anything goes'.

This is where people go.

They just go to another site, and continue sharing the violent content that big tech companies would flag.

8

#### So what?

2 reasons to be concerned about the chilling effect on speech I describe earlier:

a. For Incels, or other 'radical' individuals, online spaces that value depravity as a currency encourage a buy in to encouraging worse behaviour. When incels move from reddit to 8chan, they engage in a far smaller, non porous online bubble which is far more radical than their former community. These communities demand sinking to their level, and seeing how low one can push the bar, as it attacks community praise, recognition, and awareness. Hate speech never went away. Child pornography never went away. It went to a place that the government can never regulate, with the same people who would otherwise engage with the content contuing to. At best, this policy protects nobody. At worst, the more that these offenders who create 'harmful content' move to the 'online black market', normalization of extremism in these spaces makes them worse off and more likely to offend in these behaviours without they eye of friends, family, the public, or Facebook- to flag this behaviour as not normal, and not okay.

b. For activists and educators, they're forced to find new websites or online platforms to engage. While this doesn't seem like a harm *prima facie*, it is when you think about the role that this activism serves. It makes it harder for internet users to find the online space they desire when it isn't on a familiar, accessible social media site. First, fewer activists may find their online community or space in the first place when it's not on an accessible social media platform. Second, activists lose access to the general public, who are important in improving awareness of issues. The general public are potential allies, potential voters, potential donors, or potential future activists themselves.

Making major OSCs responsible for the actions of their users means that many vulnerable people (at risk of engaging in harmful ideology and behaviours and activists) become liabilities for the platform, and end up being silenced --- beyond the point of chilling effect--- to leaving and going somewhere else. This solves nothing and results in worst outcomes for both groups- both are groups that this policy aims to address, but leaves behind.

#### 5. Public Access

This is a penultimate public interest issue. Nearly every Canadian uses the internet and some rely on the internet for essentials: their income, connection with family and friends, connection to information, connection to entertainment, and finally personal speech and public expression.

I am shocked and concerned that for such a *powerful* policy, the public engagement for this draft action looks like: sending an email, and access to two fairly long government papers.

Short points on how the policy works would be great. Most Canadians do not have the *time*, the literacy, nor the patience to read government draft publications. They are drab, lengthy, and confusing. It takes a fairly high level of policy literacy to understand what's really being proposed here.

I learned about this policy from a fairly unflattering but useful article that explained how the policy could operate point form, what other internet regulation bills the liberals have recently proposed, and what a few major critics (all Canadian law professors) had to say on the subject. I found this article more concise and useful than the painful policy literature your website hyperlinks to.

On emailing, I think this also results in largely constructive feedback. Who are the people that write letters? Who are the people, that without a prompt, will "share their thoughts" on complex policy legislation? It's not the general public, that's for sure. It's likely not even light supporters who find the policy 'kind of neat'. I worry the responses you will get, from the people who read the technical paper, responded to the general operation of the policy, and could in anyway articulate opposition or insight beyond the surface level reasons for why we should enact this policy are people like me that find

this policy atrocious. I hope that whoever is reading this takes this in the most constructive way possible. If you want to get a better assessment beyond disgruntled legal professionals and internet denizens like myself, and a picture of most Canadians that use the internet, please have a better process for engagement.

I would strongly recommend surveys, with pointed questions and either multiple choice or scales for strongly disagree/ strongly agree. This will give you a clearer sense of peoples values, which can be complicated, and heterodox. You can also provide the option to comment, for people like me to share what my experiences with online flagging and censorship look like. Not only will more people have time for that (this is the first email I've written for feedback on a policy, yet I've done *hundreds* of municipal and provincial surveys), but people will get a better, clearer understanding of what you're proposing.

People are mad, they're scared, they're upset, they're worried.

They're mad about the rise in terrorism, that their children could be exposed to online violence and radicalizing community spaces, or unconsensual pornography of them that exists online forever.

They're scared that they could be the target of revenge porn for sharing intimate pictures, they're scared they'll see a loved one entrench themselves in the wrong space, they're scared that their news sources are no longer accurate.

In a country that has historically failed in most regulatory policy to deal with online platforms at all, which is all bark and no bite- this policy is all bite. If Facebook and YouTube decide to continue servicing Canadian IPs despite our small market share representation, and high liability cost under this motion- they will be worse online spaces in general. I'll certainly miss the good old days before I finally purchase a VPN, do my best to find trails of the communities I once valued, and curse the current Liberal government for trying to score political points off of peoples' uncertainty with an internet illiterate policy fashioned by people who don't' know what the internet means to the rest of us.

Sectorial constraints for the contract of the sector for the formation of the operation of the operation of the contract of the sector of t

s.19(1)

## Felicia Mazzarello

From: Sent: To: Subject: Dan Mazur August 14, 2021 5:02 PM ICN / DCI (PCH) Please defend and nurture small, independent OCSPs

**Categories:** 

Steven

Dear Digital Citizen Initiative,

I am writing out of concern for the government's proposed approach to addressing harmful online content.

I am worried that the proposed regulations will fail to address their stated goals because they will make online communities more dependent on big tech companies and their over-broad content moderation tools. Instead, we could have regulations that help reinforce the internet as a place where smaller communities are empowered to self-organize, independently of big tech, and moderate content according to their own standards. The proposed framework imagines that all OCSPs are 'major platforms', neglecting to even mention the small, self-organizing communities that have always existed on the internet independently of big platforms. The regulations pose a risk of entrenching the mainstream OCSPs by demanding regulatory requirements that can only be satisfied by large companies with substantial resources.

Not all online communication service providers are large companies that can staff full time content moderators or afford automated content moderation tools to deal quickly with problematic content. There are open source software platforms, such as mastodon or diaspora, that allow anyone with a bit of technical know-how to create an online communication service by installing freely available software on their own server. So, some online communication service providers are not big companies, just individuals volunteering some of their free time to help build communities online.

These small, independent platforms are very important for communities to stay independent from big tech. Individuals or groups can create safe, inclusive, and open online communities for their members that are not possible to create on a platform that aims to serve millions or billions of users, usually under a surveillance-based business model. Mastodon and diaspora are federated platforms, meaning that users on separate OCSs can interact with one another no matter which OCSP they choose (<u>https://en.wikipedia.org/wiki/Fediverse</u>). This makes it possible for users to choose their favourite service provider and still get a global experience such as the ones provided by the incumbents like Twitter or Facebook. When an individual user or a group doesn't like the content moderation policies or enforcement provided by their service provider, they can choose to migrate to a different service provider without loosing access to the broader federated community. This federated approach allows small, self-organizing communities to establish their own policies and enforcement around harmful online content without relying on a one-size-fits-all content moderation approach from a giant company trying to serve the needs of a billion users.

In the discussion guide, it is clear that "the concept of online communication service provider is intended to capture major platforms, (e.g., Facebook, Instagram, Twitter, YouTube, TikTok, Pornhub)". However, the definition given for online communication service provider in the technical paper makes no distinction between 'major platforms' and an OCS run by an individual with a handful of users, for example. The definition that is used in the technical paper is: "a service that is accessible to persons in Canada, the primary purpose of which is to enable users of the service to communicate with other users of the service, over the internet. It should exclude services that enable persons to engage only in private communications."

If a small online community is subjected to the industrial regulations described in the technical paper, a very likely outcome is that they will be unable to bring their community into compliance, become worried about facing harsh legal consequences, and will migrate their community to a mainstream service provider who can afford round-the-clock moderators and automated moderation tools. In that case, the dominance of the mainstream service provider is reinforced and the independent community loses their ability to have technological self-determination and to moderate their community standards.

I am also greatly concerned about how the mainstream service providers will comply with these regulations. In practice, the regulations will result in content moderation that is provided by automated software and poorly-trained human moderators that will be acting to protect large companies from liability. They will not be concerned with upholding lawful free speech, or defending marginalized voices. Voices that are already marginalized on the mainstream platforms will become even more marginalized, and smaller OCSPs that may have accepted them will start to vanish. I agree with the criticisms of the approach explained by the Electronic Frontier Foundation and Michael Geist, which I will link to rather than repeating here:

#### https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/

https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filtering-blocking-and-reportingrules-1

The proposed regulations will make it much more difficult to operate independent online communities. I think the goals of the regulations would be better served by making it easier. First, please ensure that any industrial regulations intended to apply to 'major platforms' explicitly exclude small, independent, online communities. The distinction must be made according to the size of an OCSPs community or to its business model, not to a technical description of the service provided. Second, make it easier for individuals and groups that are dissatisfied with the content moderation practices of mainstream providers to leave the mainstream platform. Large platforms aren't large because users love them, but because users can't interact with their friends and family except through a walled-garden platform. Leaving would be much easier if users could use a preferred platform and still interact with their friends and family on the mainstream platform as easily as they can send email to users of different email providers. This idea is called interoperability. Interoperability should be required of large OCSs. Facebook achieved its early success by allowing interoperability with the then-dominant MySpace. Please see this article for more information on the importance of interoperability: <a href="https://locusmag.com/2021/07/cory-doctorow-tech-monopolies-and-the-insufficient-necessity-of-interoperability/">https://locusmag.com/2021/07/cory-doctorow-tech-monopolies-and-the-insufficient-necessity-of-interoperability/</a>

Thank you for considering these points.

Regards, Dan Mazur

Dischardel entrolectific constituent data and base of the addition of the operation of the addition of the second of the second of the the second of the

s.19(1)

## Felicia Mazzarello

From: Sent: To: Subject: Melissa D August 13, 2021 5:39 PM ICN / DCI (PCH) Digital Citizen Initiative

Cathy

Categories:

Hello,

My name is Melissa and I started a not-for-profit called	(link to site here) in support of
cyber security for our female youth in particular advocating for proper policy changes	

I want to share two girls' experiences in regards to the need for cyber security, verification of users and educational resources for parents, guardians and caretakers of victims.

My next story is about a girl a man named Jared Nolan victimized, <u>here</u> is the Barrie News report regarding what he had done in Alliston, ON. I quote: "*The victim, who cannot be identified, told the court in a victim impact statement that it is, "difficult to be around people. I've been impacted with education and social anxiety.*" Along with what

was caught by her parents and police, there had been more images and chats deleted when the police were able to obtain his computer/devices. This is unacceptable considering it was tax payers' money he was using for solicitation. This is unfair for police as they cannot do their job diligently without obtaining the evidence that is required from the platforms they used. This sparks the rage in any parent, to think that we, as Canadian citizens who pay taxes into the system that is supposed to uphold our protection and safety, cannot due to a private corporation's legal rights. Why are the rights of corporations such as Instagram upheld before those laws that protect our dignity of our citizens?

My fundamental freedom is to protect my children, and my dignity in this country is infringed upon when I am not given the ability to protect my children from harm. The harm now done is not in bars, it is on the internet over chat, over forums, and in other places unknown to those who do not commit crimes. If there is anything I can do other than write this email and push my ideals to my community. Please let me know as this is extremely important to me.

Thank you for reading.

Regards, Melissa D'Alimonte

Michaeld - online process and states of the state of an antibolic states of the state of a state of the state of the states.

s.19(1)

## Felicia Mazzarello

From: Sent: To: Subject: Galen Fogarty August 12, 2021 8:13 PM ICN / DCI (PCH) Feedback - Proposed approach to address harmful content online

Hello,

I am writing to offer my feedback on the proposed measures to address harmful online content, and to urge an approach that is less restrictive to small organizations and individuals, which provides more protections to Canadians from government administrations which would abuse elements of this plan, and which takes into account the bad faith abuses that this sort of reporting system will invite.

In short I think large OCSPs should be regulated, but these are bad guidelines and will lead to bad laws. The monopoly power that large corporations enjoy, and their ability to control so thoroughly how content is served to users is the reason harmful content spreads so rapidly, and these guidelines cement monopolies by imposing unreasonable burdens on individuals and small organizations. Huge American and Chinese companies will be the only ones able to afford the moderation and data retention requirements mandated under these proposed laws, drastically limiting the alternative methods of communications Canadians might turn to. I think these laws would effectively destroy creative and casual uses of the technologies they govern, while giving an absolute gift to bad faith actors intent on silencing whatever speech or content they desire.

At length, I am including a rough list by item number in the technical document shared on the Canadian Heritage website of some of the areas where I think this proposal will fail in its stated purpose and impose a burden on Canadians using OCSs in good faith:

10. Automated content filters and moderation services: There is no provision in this document that any system implemented would meet any technical or quality requirements. This could easily lead to OCS users incurring the burden of proving their innocence to impenetrable automated systems or uninterested customer support departments when their content is flagged.

11. Requiring a response to flagged content within 24hrs is unreasonable to expect from any but the largest corporations. No hobbyist hosting an online forum, non-profit group making use of open software, or small competitor to major social media companies can be expected to provide this level of responsiveness. Even large corporations will be incentivized to make all flagged content inaccessible as a first step in the moderation process to avoid penalties.

12. The guidelines provide little protection against abuses of the reporting system. Specifically, bad actors intent on silencing reasonable speech or content will become experts at using the system, while regular users will be left to figure out whatever layers of policy large corporations are compelled to put in place. This will absolutely work to the detriment of the protected groups named in item 1.C.

14, 15, and 23: The type of retention policies and systems described in these items are expensive and require specialized knowledge to maintain. Again, none but the largest corporations can be expected to retain this type of information in a meaningful way, let alone keep that data safe. This proposal is effectively encoding the monopoly large social media companies already enjoy into Canada's laws. Since these guidelines are a response to a rise in harmful content pushed out by large corporations, this seems like a mistake.

17. Tailored requirements for specific types of OCSs should be specific in the guidelines that shape the proposed legislation, and in the legislation itself, not left to the discretion of the Digital Safety Commissioner of the moment.

Specifically, small organizations and individuals are more vulnerable to bad faith reporting and government overreach under these proposed guidelines.

23. Requiring record keeping to begin "...from the moment the content is identified or flagged as prescribed content on their respective OCSs" will be impossible for many administrators. The record keeping required by this guideline is effectively infinite and no protections against abuses to the reporting system are specified.

29. This language seems like it is meant to protect certain vulnerable groups, but OCSs are incentivized to treat everyone with equal harshness to avoid the penalties described in the proposed act. Groups named in item 1.C.using the OCS in good faith will be the targets of coordinated reporting by bad actors with no real stakes in the reports they are making, but OCSs will be compelled to treat these reports as legitimate.

42. The appeals process for OCSs and users of OCSs is not robust enough to protect Canadians. The number of complaints an OCS could face is not limited in a real way under the reporting system being proposed, and a government office could easily be overwhelmed by the volume of appeals required. Further, no mention is made in these guidelines about the ability of an OCS or user of an OCS to continue to host/have hosted any flagged content while a decision is being reached by the appeals panel. And neither is there any mention about potential penalties for OCSs who continue to host flagged content while a decision is in process.

46. The additional layer of an advisory council does little to protect Canadians from a government administration that would seek to abuse these legal powers when all members of the council serve at the pleasure of the ruling party.

54. "... the OCSP would then decide whether to make the content accessible or not, subject to their own guidelines." If this proposed Act is taking OCSPs as regular and powerful elements in modern life, then why is this clause in here? What would motivate an OCSP to ever host content that had been flagged when it is only a liability under these guidelines?

66 - 75: Regulatory Charges and Advisory Board. None of the language here is strong enough to stop this law from being abused by individual regulators or the administrations that appoint them.

Please reconsider the proposed approach to this problem and focus instead on limiting how monopoly corporations are able to serve radicalizing content to users by controlling and tracking the whole of their digital experience.

Thank you, Galen Bourget-Fogarty

Sochasti and Style constants Also a Sic And Anadatasi Managatha tao ang ang Si Managatha tao ang ang Si Managatha tao ang ang Si Managatha tao ang Sic Managatha tao ang Sic

### Felicia Mazzarello

From: Sent: To: Subject: Drew Wilson August 4, 2021 5:15 PM ICN / DCI (PCH) Re: Addressing Harmful Content Online s.19(1)

**Categories:** 

Alyssa

Hello,

I am writing to you in response to the online consultation about harmful content.

My name is Drew Wilson. In 2004, I started taking an interest in digital rights and began following the developments as they happened in Canada. I followed the copyright, patent, and privacy debates. In 2005, I took up the act of journalism and began writing about the events, analyzing these issues on Slyck and, eventually, ZeroPaid. In 2013, I founded to carry on this endeavour at my own pace and continue to write news articles impacting digital rights around the world, not just in Canada.

As such, I have witnessed first hand both the enormous benefits the Internet brings and the pitfalls that we encounter over a very long period of time.

It's one of these pitfalls that the online harms debate wishes to address. With the consolidation of people on larger platforms like Twitter and Facebook, what does one do about the problems of harmful, hateful content and misinformation? The negative impacts are obviously well documented. From the suicide of Amanda Todd to the January 6<sup>th</sup> insurrection of the US Capitol to the harassment of visible minorities and members of the LGBT community to the vaccine misinformation (which many have cited as a reason for the slow uptake on vaccination rates in the US), online content has an impact on the real world and real people.

Of course, I don't just offer platitudes of saying the right thing.

With having seen others start up small websites and having gone through the process involved myself, I have a pretty good understanding what it's like to be an online startup myself. There are a lot of misconceptions of what the behind the scenes of a website is like.

Many believe that the web is just Facebook, Google, Twitter, and a handful of platforms out there. Therefore, if they know how those sites operate, they know everything there is to know about how the Internet works. That obviously is a really bad way to gauge how the Internet works today despite the popularity of the largest platforms.

Another stereotype often seen on TV is that a group of people in business suits rent out a whole floor in an open concept office plan. They are backed by hundreds of thousands in venture capital and the floor is filled with duel screen Mac computers with people clicking and typing away. A spokesperson is happily pointing out how they have finally been able to launch this amazing website and the future is so very bright for them.

My first hand experience is that neither of these scenarios is even close to the typical norm of what it's like to start a website for most people. For a portion of websites, they were started up because a business decided they just needed a web presence. Often, these sites are thrown together just for the purpose of ticking a box and is left as a side project to an employee who seems to know a few things about this whole Internet thing.

For many of the remainder websites, it's often anywhere between one and three people deciding they have an idea. They research hosting and domain name registration solutions, spend the hundred or so dollars needed, get those accounts running, and start largely learning on the fly. Some have a decent computer science degree or a design diploma while others are just plain learning from scratch. Will the website take off? Will it fail? Who really knows? After all, Google started as a couple of servers sitting in someones garage and now they are a multi-billion dollar giant. You never really know if an idea can take off or not. Some may not even start a website in the hopes of making it big. Rather, it's just a small project for a couple of friends or a group of people. Others are just putting together a site for portfolio purposes.

Put simply, the Internet is huge. The number of sites that exist so often measures in the billions and the number of active sites measures in the hundreds of millions. At best, any one person will have a cursory understanding of what the Internet is like. It is impossible to fully comprehend the full extent of what the Internet is today. You can only really take in a tiny patch of the digital space today.

It is with this in mind that when we talk about regulation on the Internet, there are a couple of fundamental questions we need to ask. This includes:

- 1. Is this regulation really feasible?
- 2. Who is this regulation targeting?
- 3. Will it harm the overall Internet ecosystem either directly or indirectly through unintended consequences?
- 4. What will the impact be on people?

Trying to implement good regulation on the Internet is notoriously difficult. Between the stakeholders with competing interests and dealing with different political ideologies and even the technical aspects of how technology really works presents an absolute minefield for where legislation can go wrong. Very few regulations have really worked well. Some success has been seen with network neutrality laws and even some privacy laws like those found in Europe. A vast majority of laws that have negatively impacted are often driven by political ideological reasons or by heavy lobbying from specific stakeholders. An example of the former is the US debate surrounding Section 230 reformation and an example of the latter is the numerous copyright reform laws and legislation.

After seeing countless laws being debated over the years around the world, the looming online harms legislation seems destined to fall within the former category. As someone who is hoping to make an impact on the Internet in a positive way, I find it also incredibly troubling despite the problems it hopes to solve being very real problems.

According to the technical paper, the government wants to tackle 5 forms of harmful content. This includes terrorist content or content that actively encourage terrorism, content that might incite violence and hate speech.

For terrorist content, the problem with that is that what constitutes terrorism is always changing. For instance, during the Harper government, there was a push for define some forms of environmental activism as "eco terrorism". Mercifully, that didn't come to full fruition, however, there was motivation to do so. Furthermore, there have been instances where private companies or individuals try to define the lawful conduct of a person or group as terrorism as well. So, this raises the question, "If the definition of 'terrorism' is constantly changing, how do you expect website's of all shapes and sizes to really keep up?" After all, this legislative push wouldn't just theoretically be here with the norms of the government of today, but all future governments as well.

For violence or the threat of inciting violence, this is also an extremely loose thing and one I actually witnessed on a website called Techdirt. There was an article about a controversial judge and the patent system. Apparently, that caused someone to comment with the following:

"Hell, eventually somebody might decide that it's cheaper to pay a hitman to just cut a brake line or something than go through discovery in that judge's court. "

While this is, indeed, a rather salty comment, it's not necessarily advocating violence. However, it was enough for the US Marshals to demand that the comment be preserved internally along with all information held by the site. The investigation didn't move forward and a gag order on what happened was released. This alone highlights why policing content advocating violence is not going to be easy by any means.

Hate speech, of course, is not going to be any better. If someone decides to simply offer a comment as an illustrative example, then does that constitute spreading of hate speech? The obvious answer is that it depends on the context. At that point, the question is, where does one draw the line on that?

To return to the four questions I listed above, is this really something that can be pushed feasibly? Even on a well moderated site, we are already, at minimum, on shaky grounds as it is.

Things start to get worse with the second question: who is the regulation targeting? The technical paper defines this with the following in the second and third paragraph:

"The Act should define the term Online Communication Service (OCS) as a service that is accessible to persons in Canada, the primary purpose of which is to enable users of the service to communicate with other users of the service, over the internet. It should exclude services that enable persons to engage only in private communications.

The Act should provide that the Governor in Council may, after consultation with the Digital Safety Commissioner, make regulations (a) excluding a category of services from the definition of OCS; (b) specifying a category of services that is to be included by regulations, notwithstanding that it does not meet the definition of OCS, if the Governor in Council is satisfied that there is a significant risk that harmful content is being communicated on the category of services or that specifying the category of services would further the objectives of this Act; and (c) respecting the meaning of the term private communications for the purposes of the definition of OCS."

While there have been examples laid out that says that platforms like Facebook, TikTok, and Twitter would qualify, the paper is clear that it is far more broad than this. It's basically any and every website online that supports comments. It is clear that any website that supports a web forum is under this legislation. Wordpress, which is a CMS used by a huge variety of sites, supports comments as well. The only kind of site I can see not falling into the category of sites that would be regulated might be static web 1.0 websites built entirely out of HTML and CSS. If you make a website that says "hello world", you probably will be safe. For everyone else? As far as I can tell, you'll probably be under this regulation sooner or later. This isn't even getting to the really complex communication methods of utilizing a third party service like Disqus where I wouldn't even begin to be able to figure out what the site has to do to be compliant with the law.

If there is any doubt about this interpretation, paragraph 6 removes this doubt:

"The Act should ensure that it applies to all regulated Online Communication Services (OCSs), and Online Communication Service Providers (OCSPs) that are the closest legal entity to a regulated OCS, that provide services to peoples in Canada. "

So, to answer the second question, the proposed law as described in the paper appears to be targeting almost everyone who operates a website. This adds to the tenuousness of the feasibility of what is being proposed here.

We next find ourselves moving to our third question: "Will it harm the overall Internet ecosystem either directly or indirectly through unintended consequences?"

This nicely align with what we see next in the technical paper. Paragraph 10 states:

"The Act should provide that an OCSP must take all reasonable measures, which can include the use of automated systems, to identify harmful content that is communicated on its OCS and that is accessible to persons in Canada, and to make that harmful content inaccessible to persons in Canada, as may be prescribed through regulations by the Digital Safety Commissioner, on approval by the Governor in Council.

a. The Act should provide that an OCSP must take measures to ensure that the implementation and operation of the procedures, practices, rules and systems, including any automated decision making, put in place for the purpose of moderating harmful content that is communicated on its OCS and that is accessible to persons in Canada, do not result in differential treatment of any group based on a prohibited ground of discrimination within the meaning of the <u>Canadian Human Rights Act</u> and in accordance with regulations. "

"[A] The Act should provide that an OCSP must address all content that is flagged by any person in Canada as harmful content, expeditiously after the content has been flagged.

a. [B] The Act should provide that for part [A], "expeditiously" is to be defined as twenty-four (24) hours from the content being flagged, or such other period of time as may be prescribed by the Governor in Council through regulations."

While this is already an extremely high bar, paragraph 11 makes this additional stipulation:

"[A] The Act should provide that an OCSP must address all content that is flagged by any person in Canada as harmful content, expeditiously after the content has been flagged.

a. [B] The Act should provide that for part [A], "expeditiously" is to be defined as twenty-four (24) hours from the content being flagged, or such other period of time as may be prescribed by the Governor in Council through regulations."

So, anyone at any time can make a complaint. This already adds an incredible burden on website owners as it is. What's more is that we see this for paragraph 12:

"[C] The Act should provide that an OCSP must institute internal procedural safeguards providing users of the service in Canada with the following, as may be prescribed through regulations by the Digital Safety Commissioner, with the approval of the Governor in Council:

- a. accessible and easy-to-use flagging mechanisms for harmful content;
- notice of the OCSP's content moderation decision within twenty-four (24) hours of the content being flagged, unless the timeframe is changed by the Governor in Council;
- c. the accessible and easy-to-use opportunity to make representations, and compel an OCSP to promptly review and reconsider its decision; and
- d. notice of the OCSP's decision upon reconsideration, which must be provided without delay, including a notice of the recourse available to the Digital Recourse Council of Canada. "

I wouldn't even know where to begin with trying to be in compliance with this. As a result, I find myself wondering if my site has a future under these heavy regulations. This further raises the question, "If someone who actually follows these issues can't even begin to figure out how to be in compliance, what about the millions of others who don't even have my level of experience with these issues?"

Where things really start flying off the rails, however, is paragraph 14:

"The Act should provide that an OCSP must generate and provide reports on a scheduled basis to the Digital Safety Commissioner on Canada-specific data about:

- a. the volume and type of harmful content on their OCS;
- the volume and type of content that was accessible to persons in Canada in violation of their community guidelines;
- c. the volume and type of content moderated;
- d. resources and personnel allocated to their content moderation activities;
- e. their content moderation procedures, practices, rules, systems and activities, including automated decisions and community guidelines;"

That is combined with paragraph 15:

"The Act should provide that an OCSP must maintain records as necessary for the proper administration of the Act, in accordance with the requirements set out in the Act or prescribed through regulations by the Digital Safety Commissioner, or as otherwise required by law."

To say that any website can comply with 14. (a) in this paper is extremely unconvincing. What qualifies as harmful content and what doesn't qualify as harmful content may differ from person to person. The ask is to quantify content that is subjective. As far as I'm concerned, no website in existence today is adequately capable of producing this. In short, the government is asking the practically impossible.

Of course, the harm extends beyond just website operators. Paragraph 14 (c) combined with paragraph 15 suggests that all comments be preserved in the event that the Digital Safety Commissioner comes knocking. As anyone who operates a website in any reasonable amount of time knows, even the government actually does not want that. The simple reason is in one word: spam. Does the government really want the records of, for me personally, approximately 2.3 million spam comments? I find that highly unlikely. That would do neither side any good unless web administrators want to utilize this as a form of protest.

Further, paragraph 26 suggests that when a website administrator is forced to send information to the RCMP, not to disclose this report:

"The Act should provide that an OCSP must not disclose that it has (a) issued a notification to the RCMP or (b) issued a report to law enforcement and CSIS or disclose the contents of (a) a notification or (b) a report, if the disclosure could prejudice a criminal investigation, whether or not a criminal investigation has begun. "

This opens up the possibility that criminal records are made of people without their knowledge. As awareness is raised about a theoretical law that requires this, it only serves to encourage anonymous communications. For most rational people, if they have a choice between using the TOR network or a VPN service versus unknowingly getting a criminal record, they will choose the TOR network or a VPN service. While I don't know much about how CSIS operates, I'm pretty sure that if they had a choice between a simple communication and peeling open the layers of the Onion network (TOR) for that same message, they would rather choose the former for resource purposes alone.

To answer to the third question, as a result of all of this is, yes, it will harm the Internet ecosystem both directly and indirectly. It also answers the fourth question, "What will the impact be on people?". The answer is, "substantially bad".

First of all, everything about this strikes me personally as overly burdensome. For a lot of this, I can't figure out what technical solution would even come close to allowing my website to comply with these regulations. Quite frankly, I can't even begin to fathom a solution that would be capable of complying with something this subjective. I'm only one person. When I see paragraph 119 talk about \$20 - \$25 million fines, I don't even honestly know if it's even possible for me to maintain my website. For anyone who has less technical expertise than me, they probably don't even stand a chance staying in business or keeping up their site. The threat of fines like this will not only deter people of today to continue operating websites, but will also deter people from making new online startups in the future. It is not in the interest of Canada to block the starting of a Canada made tech giant of tomorrow. Further, it is not in the interest of Canada to send a message that Internet innovation is not welcome in this country – which is a message that is made so loudly and clearly in this technical paper.

For smaller players like me, the only viable option I see at this stage is to close up shop. If smaller players can't even have a hope of starting up something, the Canadian government will have effectively banned entrepreneurship not backed by significant sums of money from the outset.

For larger players all the way up to the tech giant's, the scale immediately becomes the problem. Sooner or later, there will be a slip-up. The multi-million dollar fines will immediately bankrupt the medium players easily.

For larger players, a serious question will be asked, "Is it worth it to risk regular fines?" Eventually, the answer will be "no". It will be cheaper just to geo-block Canada than to comply with regulations this hazy.

What does this leave us? Canada effectively shutting down the entire Canadian Internet. I don't think I even need to explain the devastating economic impact that would have on Canada. It is self-evident. If I were a visible minority or the subject of online hate for, say, sexual preference, I would find the idea shutting down the whole Internet in my name infuriatingly insulting. It is the equivalent of stopping road rage by destroying every road in the country. Does it solve the road rage problem? Well, you can't have road rage without roads. It's a solution that harms everyone and takes the approach of using a sledge hammer to squash a mosquito.

In conclusion, this whole paper is a terrible idea. It basically envisions that web administrators can wave a magic wand and magically make "harmful content" magically disappear. It would be incredibly misguided to think that regulation will somehow spawn innovation out of thin air in this context. When a reasonable solution isn't available, it simply isn't available. Should this paper become legislation and move forward and become law, we are only going to see mass closures of any business that relies on web infrastructure. Thanks to COVID-19, that is going to be a lot. So, for the sake of me and everyone else hoping to get a business start on the Internet, please do the right thing and toss this whole thing in the trash where it belongs.

Thank you,

- Drew Wilson

Founder of Freezenet.ca

Dercramment permitten synon a o (14) sur l'acola d'Infinition ADD VERY ARROW AND A COMPANY A C the Access in Wastmatter Link.



BAR ASSOCIATION L'ASSOCIATION DU BARREAU CANADIEN

# Legal Remedies for Victims of Hate Speech

**CANADIAN BAR ASSOCIATION** CONSTITUTIONAL AND HUMAN RIGHTS, CRIMINAL JUSTICE AND SEXUAL ORIENTATION AND GENDER **IDENTITY COMMUNITY SECTIONS** 

September 2020

Seathards - construction to seath to exist on Pacific Systematic and the seather seath of the seather seather to seather seather seather seather to seather seather seather

# PREFACE

The Canadian Bar Association is a national association representing 36,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the CBA Constitutional and Human Rights, Criminal Justice and Sexual Orientation and Gender Identity Community Sections, with assistance from the Advocacy Department at the CBA office. The submission has been reviewed by the Law Reform Subcommittee and approved as a public statement of the CBA Constitutional and Human Rights, Criminal Justice and Sexual Orientation and Gender Identity Community Sections.

Descriming commonly on an annual pri la (17) sur Pacchy & Calling annual Regionest) asses and common 2 the Access (5-Macminist Acc

# TABLE OF CONTENTS

# Legal Remedies for Victims of Hate Speech

۱.	INTRODUCTION1		
ıı.	AC	A CIVIL REMEDY1	
	Α.	Due Process	
		1. Costs	
		2. Screening	
		3. Election of forum	
		4. Parties	
		5. The right to know your accuser 6	
		6. Disclosure7	
	В.	Contempt	
	C.	A specific online hate remedy8	
ш.	AC	RIMINAL REMEDY 10	
		1. Consent of the Attorney General 10	
		2. Religious expression 12	
		3. No safe harbour provision 12	
		4. Private conversation 13	
IV.	от	THER OPTIONS14	
	Α.	Addressing the gap in data collection and tracking online hate 14	
		1. The police 14	
		2. The public 15	
	В.	Formulating definitions of hate 15	
	C.	An international treaty 16	
	D.	Ongoing consultation17	
v.	со	NCLUSION	

Analisista construction construction A.C. O.S. Call of antibusis Analysistation construction (Analysistation construction) (Analisistation construction)

# Legal Remedies for Victims of Hate Speech

# I. INTRODUCTION

The Constitutional and Human Rights, Criminal Justice and Sexual Orientation and Gender Identity Community Sections of the Canadian Bar Association (CBA Sections) are pleased to comment on Justice Canada's consultation paper dated July 14, 2020.

Canada needs principled and effective civil and criminal legal remedies to combat online hate that balance the right to freedom of expression with the right to freedom from incitement to hatred and discrimination. Putting too much weight on freedom of expression unduly hampers the law against incitement to hatred, while putting too much weight on combating incitement unduly restricts the right to freedom of expression.

In Canada, we have had the misfortune of getting this balance wrong both in the civil and criminal law. The application of the criminal law leans too heavily in the direction of protecting freedom of expression, inhibiting efforts to combat hate speech. The civil law had leaned heavily in the direction of combating incitement to hatred, to the point that it was repealed for its undue inhibition of freedom of expression.

The CBA Sections are pleased that the Government of Canada is taking a fresh look at these laws and has a renewed chance to get the balance right. Like the consultation paper, our submission addresses general issues with a focus on online hate. Our comments consider civil and criminal law remedies and some of the other options identified in the consultation paper.

# II. A CIVIL REMEDY

The Criminal Code is a general legal instrument for combating online hate. Criminal law is often an inadequate tool as the standard of proof is too high, the remedy of criminal punishment is often inappropriate, and enforcement is by a general criminal system rather than an expert human rights system.

While the CBA's Constitutional and Human Rights Law Section and Equality Committee supported the former section 13 of the Canadian Human Rights Act (CHRA)<sup>1</sup>, the CBA Sections

Bill C-304 Canadian Human Rights Act amendments (hate messages), Canadian Bar Association Constitutional and Human Rights Law Section and Equality Committee, 2012.

recognize that concerns about the provision and its use led to its repeal. We recommend modifying the text of the former provision to offer greater procedural protections. With these changes, the civil remedy would more effectively balance protecting freedom of expression and combatting hate speech.

# A. Due Process

The repealed section 13 of the CHRA was substantively sound but procedurally defective, leading to an undue limitation on freedom of expression. How do we prevent the easily offended from shutting down legitimate expression? How do we stop perpetrators from purporting to be victims and attempting to use the law to silence criticisms of their incitement by claiming that the criticism is incitement? Our answer is to reenact the substance of the former section 13 of the CHRA with additional procedural safeguards, so that the law does not become a vehicle for the harassment of legitimate expression as the previous section had been.

### 1. Costs

One element of justice is equality of arms. Where human rights commissions interpose between complainants and respondents, complaints are cost-free while respondents may be put to great expense. There is no equality of arms.

Criminal complaints are different because of the strict rules of evidence and high standard of proof. There is a lower bar for a defendant in a criminal investigation to avoid proceedings compared to a respondent in a civil investigation.

Once a Commission begins an investigation, exoneration requires effort and expense from the respondent. The maxim of innocent until proven guilty beyond a reasonable doubt does not apply. While the onus in civil proceedings falls on the asserting party, a small matter can tip the balance of probabilities from one side to the other when evidence is evenly matched. Respondents ignore complaints at their peril.

In civil proceedings in superior courts, costs generally go with the cause, which prevents litigation from being undertaken lightly. This is more than a brake on frivolous proceedings. Costs are awarded against the losing side even where a motion to strike for no reasonable cause of action fails and the case has some merit but not enough. When a party knows that the financial loss in an unsuccessful case is substantial, they will think twice before commencing or defending the proceedings. Submission of the Constitutional and Human Rights, Criminal Justice and Sexual Orientation and Gender Identity Community Sections of the CBA

Courts have the discretion not to award costs against an unsuccessful litigant where an issue of general significance is addressed and resolving it is a matter of public interest. Rather than relying on the common law of costs, legislation should set out principles relevant to the award of costs in proceedings before the Tribunal. Under these principles, meritorious complaints addressing matters of public interest are not inhibited, but the procedure does not itself become a form of harassment (e.g. repeated frivolous complaints), or evasion (e.g. defenses lacking merit.)

The Canadian Human Rights Tribunal needs to have the power to award costs against both individual complainants and the Commission in cases where it has assumed conduct of a case. The Tribunal should also have the power to require security for costs against individual complainants in cases where the Commission does not assume conduct of the case.

In 2011, the Supreme Court of Canada decided that the Canadian Human Rights Tribunal did not have the power to award costs under its statute.<sup>2</sup> The CBA intervened in that case argued that the principle of access to justice required an interpretation of the CHRA which would include reimbursement for legal costs.

Costs can be awarded where it is allowed by legislation. For instance, British Columbia's Human Rights Code gives the Human Rights Tribunal the power to award costs in several circumstances including against a party who engaged in improper conduct during the course of the complaint.<sup>3</sup> We recommend amending the CHRA to give the Tribunal express power to award costs against all complainants and respondents and order security for costs against all except the Commission.

#### 2. Screening

Human rights commissions have been overwhelmed by complaints. Investigating and conducting these cases have caused substantial delays. In British Columbia, the response to this was to first abolish the Commission and then reinstate it in 2018 without the power to screen or assume conduct of complaints to the Tribunal.<sup>4</sup> In Ontario, the Commission survived, but has been taken off case work, with a couple of exceptions. The Commission initiates applications at the Ontario Human Rights in the public interest with a focus on systemic issues. The

<sup>&</sup>lt;sup>2</sup> Canada (Canadian Human Rights Commission) v. Canada (Attorney General) 2011 SCC 53.

<sup>&</sup>lt;sup>3</sup> Section 37(4)(a)

<sup>4</sup> Progress of Bills

Commission also intervenes in Tribunal cases, when it thinks the outcome will affect a larger number of people.<sup>5</sup>

We recommend adopting these procedures for the Canadian Human Rights Commission with a variation. The Canadian Human Rights Commission should screen all complaints to determine whether to dismiss cases at an early stage. The Commission should also be able to take ownership of the investigation and pursuit of select cases as it sees fit.

The Canadian Human Rights Commission has the discretion to refuse to deal with complaints which are trivial, frivolous, vexatious or made in bad faith. If complainants can go straight to a Tribunal this power will have less significance.<sup>6</sup> Respondents should be able to bring a motion before the Tribunal at an early stage to dismiss a complaint that is trivial, frivolous, vexatious or made in bad faith.

A more specific power is the focus of anti-SLAPP [Strategic Lawsuit against Public Participation] legislation, which now exists in Ontario, British Columbia and Quebec. In September 2020, the Supreme Court of Canada reaffirmed the constitutionality of this legislation.<sup>7</sup> We suggest adopting a test drawing on Ontario's legislation. It should include a determination of whether the harm suffered or likely to be suffered by an individual or the public interest as a result of the expression is sufficiently serious that the public interest in permitting the proceeding to continue outweighs the public interest in protecting the expression.<sup>8</sup>

There is currently decoupling of screening and conduct of general criminal law cases. Most criminal cases can proceed by way of private prosecution without any government consent. The Crown has a choice but not a legal obligation to assume conduct of the prosecution in these cases. For some offences, the consent of the Attorney General is necessary. For others conduct by the Crown is required.

Consent is necessary for the criminal offence of incitement to hatred. Once consent is given, the prosecution can be conducted either by the Crown or a private prosecutor.

<sup>&</sup>lt;sup>5</sup> Canada (Canadian Human Rights Commission) v. Canada (Attorney General), 2011 SCC 53 (CanLII), [2011] 3 SCR 471

<sup>6</sup> Section 41(1)(d)

<sup>7 1704604</sup> Ontario Ltd. v. Pointes Protection Association 2020 SCC 22 and Bent v. Platnick, 2020 SCC 23

<sup>8</sup> Ontario Courts of Justice Act 137,1(4)(b).

Submission of the Constitutional and Human Rights, Criminal Justice and Sexual Orientation and Gender Identity Community Sections of the CBA

Regardless of whether requiring consent by the state for criminal prosecutions of incitement to hatred is advisable or necessary, it is appropriate and possibly required by the *Charter of Rights and Freedoms* in civil proceedings. The standard of proof of a balance of probabilities in civil proceedings is lower than the criminal standard of proof of beyond a reasonable doubt. The higher standard in criminal proceedings acts as a brake on frivolous proceedings. A consent requirement for civil proceedings is needed, in practice if not in law, to compensate for the lower standard of proof.

#### 3. Election of forum

It is possible to pursue essentially the same human rights complaint in several Canadian jurisdictions simultaneously. Each forum addresses the substance of the complaint without considering that the same complaint has been filed elsewhere.

Injustices accumulate when there can be multiple frivolous complaints against the same respondent and the tribunals do not have the power to award costs to the successful side. Respondents in these complaints wrack up costs fighting off the same complaint in several forums at the same time.

The CHRA provides that the Commission:

"In addition to its duties ... with respect to complaints regarding discriminatory practices ... shall maintain close liaison with similar bodies or authorities in the provinces...to avoid conflicts respecting the handling of complaints in cases of overlapping jurisdiction;"<sup>9</sup>

This section does not appear to give the Commission the power to refuse to consider a complaint on the ground that it is already being considered in another province. The provision refers to the obligation to avoid conflicts as something different from duties with respect to complaints. If this power existed, the Commission should have dismissed past simultaneous complaints on this basis, but it has not done so.

The ability to make several complaints at once in different jurisdictions against the same respondent enables a complainant to harass the object of a complaint. This avenue of harassment needs to be cut off. Complaints should be required to choose one venue. Once they

have made this choice, no other jurisdiction should be able to consider a complaint that is essentially the same.

#### 4. Parties

While human rights commissions have the power to add parties, it is not clear that they have the power to remove parties. The CHRA gives the Chair of a Tribunal the power to add parties,<sup>10</sup> but not to remove them.

Once someone is named a respondent, they remain as a respondent. The complaint itself can be dismissed on its merits. But where the subject matter of the complaint is meritorious but has been made against the wrong respondent, the complaint goes to its conclusion against the wrong complainant. The Canadian Human Rights Commission and Tribunal need to have the power to remove parties.

#### 5. The right to know your accuser

It would seem basic to the respect for human rights that a person should not be asked to answer anonymous accusations based on rumour. In his testimony before the Standing Committee on Public Accounts on December 12, 1989, then Canadian Privacy Commissioner John Grace, stated that one of the rights conferred by the Privacy Act:

"... is to know what accusations against us are recorded in government files and who has made them. Whether such accusations are true and well intentioned, as some may be, or false and malicious, as other may be, it is fundamental to our notion of justice that accusations not be secret nor accusers faceless."<sup>11</sup>

There is nothing in the CHRA preventing the pursuit of anonymous complaints. A complaint can be based on rumour, and the source of the rumour need not be disclosed to the respondent. This is a defect in the legislation and is not respectful of human rights.

There may be justification for anonymity in some cases. For instance, if there is:

(i) a serious possibility that the life, liberty or security of a person will be endangered if the identity of the complainant is disclosed,

<sup>&</sup>lt;sup>10</sup> Section 48.9(2)(b)

Minutes of Proceedings and Evidence on the Standing Committee on Public Accounts, Issue No. 20 (12/12/89), at p. 10

Submission of the Constitutional and Human Rights, Criminal Justice and Sexual Orientation and Gender Identity Community Sections of the CBA

- (ii) a real and substantial risk to the fairness of the proceeding such that the need to prevent disclosure of the identity of the complainant outweighs the interest that an accused know their accuser, or
- (iii) a real and substantial risk that disclosure of the identity of the complainant will adversely affect public security.

However, these justifications should be exceptions and not swallow the rule. The legislation should require that those who make an accusation be identified to the respondent of the complaint subject to specific exceptions.

# 6. Disclosure

There should be a general right of disclosure to the respondent in the CHRA. Currently, the text of the comments which prompted the complaint need not be disclosed to the respondent.

If the Commission seeks an expert opinion during its investigation of a complaint, that opinion legally should be available to the respondent. This disclosure is not currently required.

The CHRA should be amended to include a stated general principle of disclosure. The CHRA describes matters which should not be disclosed without stating anything about what should be disclosed.<sup>12</sup> In other federal legislation, specific prohibitions against disclosure are exceptions to a general principle of disclosure.

# B. Contempt

The repealed section 13 of the CHRA was limited not only to hatred, but also addressed contempt. The provision stated that:

"13 (1) It is a discriminatory practice for a person or a group of persons acting in concert to communicate telephonically or to cause to be so communicated, repeatedly, in whole or in part by means of the facilities of a telecommunication undertaking within the legislative authority of Parliament, any matter that is likely to expose a person or persons to hatred or contempt by reason of the fact that that person or those persons are identifiable on the basis of a prohibited ground of discrimination."

The prohibition of incitement to hatred is an international human rights standard in the International Covenant on Civil and Political Rights.<sup>13</sup> Canada is a state party to the Covenant.

<sup>&</sup>lt;sup>12</sup> Section 33(2)

<sup>13</sup> Article 20(2)

There is no comparable international human rights standard about contempt. In the *Whatcott* case, the Supreme Court of Canada reasoned that the concept of contempt was included in the concept of hatred.<sup>14</sup> In light of that reasoning, it would be simpler if the word were omitted from a re-enacted provision.

# C. A specific online hate remedy

Existing remedies not specifically addressed to the internet may be available to address online hate. For instance, section 12 of the CHRA may be available to address hate speech on the internet.

We recommend adding a remedy that is specific to the internet. This would remove uncertainty and avoid litigation about the meaning of more generic legislation. It could also serve as a warning with an educational and preventive purpose. There is a missed opportunity to have legislation serve that purpose for the internet if the legislation is silent about the internet.

A revised civil remedy needs to be directed not only against inciters, but also against publishers, including internet platforms. Internet providers should not have civil immunity for the material on their platforms.

Rather than legislating the removal of liability of internet providers from individual defamation suits, we recommend that the Canadian Human Rights Tribunal have the power to make orders which are legally binding on internet providers.

The repealed section 13 of the CHRA excluded internet providers from its ambit:

"(3) For the purposes of this section, no owner or operator of a telecommunication undertaking communicates or causes to be communicated any matter described in subsection (1) by reason only that the facilities of a telecommunication undertaking owned or operated by that person are used by other persons for the transmission of that matter."

A re-enacted section 13 should go beyond removing this provision. There should be an express provision that says the exact opposite: when an internet provider allows a person to use their services, the provider is communicating what the person posts on the provider's platform.

<sup>14</sup> Saskatchewan (Human Rights Commission) v. Whatcott, 2013 SCC 11, [2013] 1 SCR 467 paragraph 43

### Submission of the Constitutional and Human Rights, Criminal Justice and Sexual Orientation and Gender Identity Community Sections of the CBA

In their terms of service, major internet providers prohibit incitement to hatred and illegal content. When something is considered incitement to hatred, it is removed globally. When something is illegal in a particular country, it is blocked for that country.

Internet providers block content by IP address (the internet protocol address of a computer on the internet) where the law requires them to do so. IANA (the Internet Assigned Numbers Authority) assigns IP addresses by country. Blocking content in a country using IP addresses is technically straightforward.

In theory, the terms of service of the major internet providers prohibit incitement to hatred. Effort should be made to turn this theoretical prohibition into prohibition in practice.

There would be major obstacles to doing this. First, prohibiting and taking down content works against the business models of providers, which is to have as many users as possible and maximize advertising revenue. While it may be commercially advantageous for some hate speech to be taken down from a platform if it diminishes the reputation of the provider, that is not always the case. Second, providers lack expertise in hate speech. They often do not recognize hate speech when they see it. A third challenge is the sheer volume of material on the internet. Even if providers are held responsible only for problematic content brought to their attention, the volume is very large.

The European Commission addressed the problems of expertise and volume with a system of trusted flaggers. In agreement with four major internet platforms—Facebook, Twitter, YouTube and Microsoft--the Commission adopted, a code of conduct on countering illegal hate speech online. The companies agreed to review the majority of valid notifications for removing lllegal hate speech in less than 24 hours and to remove or disable access to this content, if necessary.<sup>15</sup> Organizations located in twenty seven European Union member states were accepted as trusted flaggers or reporters to notify companies of alleged illegal hate speech and report the reactions to the Commission. According to a January 2020 fact sheet from the European Commission, there are 39 trusted flaggers.<sup>16</sup>

15

16 January 2020 fact sheet from the European Commission

Code of Conduct on Countering Illegal Hate Speech, online, page 3 bullet 3.

The Canadian Human Rights Commission should reach a similar agreement with the major internet providers and develop its own list of trusted flaggers. The work should be coordinated with the European Commission and the European trusted flaggers to avoid duplication of effort. Where companies comply voluntarily, legal restraints would be unnecessary.

A fourth problem in implementing the terms of service of internet providers on prohibiting hate speech is that many of the major internet providers are headquartered in the US and are imbued with America's absolutist tradition on free speech. They often do not consider what those outside the US would consider hate speech to be a violation of their terms.

Internet providers need not have the final word on what hate speech is. The Canadian Human Rights Tribunal can make its own determination. If the Canadian Human Rights Tribunal determines that an internet communication is hate speech, the major internet providers will respect that determination for Canada, because they commit to respecting local laws. They will comply with the law in Canada even if they do not agree with the Tribunal about what hate speech is. Once a Canadian Human Rights Tribunal determines that something on a major internet provider's platform is hate speech, the provider will block that content for all computers with Canadian IP addresses. The law should empower the Tribunal to require providers to do so.

What is blocked would be effective for Canada but not globally. The existence and application of a Canadian law on online hate to Canadian territory would be a substantial advance from where we are now.

## III. A CRIMINAL REMEDY

There is a prohibition in the Criminal Code against incitement to hatred, but it is not as effective as it could be. We have identified two problems.

#### 1. Consent of the Attorney General

Generally, where the consent of the Attorney General is not required, the Crown prosecution of a crime will proceed if there is sufficient evidence to convict. Prosecutors have discretion not to proceed even where the evidence could lead to a conviction, but they must exercise that discretion according to clear principles. For instance, prosecution may not proceed if the hardship to the accused would be disproportionate to the benefit to society. The requirement of obtaining the consent of the Attorney-General before a prosecution can commence removes the possibility of private prosecution. If private prosecutions are possible, anyone could prosecute anyone else for something they said that the private prosecutor thought was hate speech. Arbitrary prosecutions are as harmful to human rights as arbitrary refusals to prosecute.

When the Crown prosecutes, it will not do so unless the prosecution believes it has evidence to establish guilt beyond a reasonable doubt. Private prosecutors need not exercise similar restraint.

If private prosecution of hate speech were possible, private prosecutors could legally launch a prosecution merely because they disagreed with the accused. This prosecution would not succeed, but it could amount to harassment of the accused.

The CBA Sections accept that the consent of the Attorney General is appropriate in this area, but consent or denial of consent must be exercised according to principle. In British Columbia, the Crown Counsel Policy Manual provides that in almost all hate offences, the public interest applies in favour of prosecution (see an excerpt of the manual attached). <sup>17</sup>

Approvals for alternative measures should be given only if:

- 1. Identifiable individual victims are consulted and their wishes considered.
- 2. The offender has no history of related offences or violence.
- 3. The offender accepts responsibility for the act, and
- 4. The offence must not have been of such a serious nature as to threaten the safety of the community

These criteria could be adopted for denial of consent. There should be guiding principles, rather than a vacuum where consent can be denied arbitrarily without explanation as is currently the case.

The exercise of prosecutorial discretion is not subject to judicial review. The courts have reasoned that if they either affirmed a decision to prosecute or overturned a decision not to prosecute, the decision might seem to favour the prosecution over the defense. To maintain an appearance of neutrality, they have declined to get involved at all in prosecutorial discretion.

17 British Columbia, Crown Counsel Policy Manual.

With the unavailability of judicial review for the exercise of prosecutorial discretion, governance must be undertaken by the prosecution itself if it is to be guided by principle. The Attorney General's grant or denial of consent for hate speech crimes should be subject to clear public criteria. Reasons should be given for the grant or denial of consent explaining why the criteria were or were not met.

2. Religious expressionThe offence of incitement to hatred in the Criminal Code sets out as a defence statements which:

"in good faith, the person expressed or attempted to establish by an argument an opinion on a religious subject or an opinion based on a belief in a religious text".<sup>18</sup>

There were differing views among the CBA Sections on this defense. Some were of the view that a defense for religious expression was not needed. As with all *Charter* rights and freedoms, if there is a conflict between freedom of religion and freedom from incitement to hatred, the rights need to be balanced against one another. Others believed that the defense was necessary so that sincerely held beliefs of religious minorities expressed in good faith are not subject to prosecution. We recommend further study of this issue.

#### 3. No safe harbour provision

The Criminal Code provides that:

"A judge who is satisfied by information on oath that there are reasonable grounds for believing that any publication, copies of which are kept for sale or distribution in premises within the jurisdiction of the court, is hate propaganda shall issue a warrant under his hand authorizing seizure of the copies."<sup>19</sup>

Even if it were modified, this provision of the Code would not be well suited to deal with hate on the internet, as it deals with material not yet communicated and anything on the internet has already been communicated. Code section 320(1) also puts the initiative on the Court at first instance, rather than the owner or occupier of premises in which the offending material is kept for sale or distribution. For internet communications, the primary responsibility should rest with the communicators, not the legal system.

Regulations under the Broadcasting Act provide that no broadcaster licensed under the Act

"shall distribute a programming service that the licensee originates and that contains ... any abusive comment or abusive pictorial representation that, when taken in context, tends to or is likely to expose an individual or group or class of individuals to

19

hatred or contempt on the basis of race, national or ethnic origin, colour, religion, sex, sexual orientation, age or mental or physical disability;"<sup>20</sup>

While the standard is worth emulating, it is not practical to fit internet providers into this framework because they are not licensed. The remedies for the enforcement of this standard include conditions on licencees and potential withdrawal of licences. For internet providers who are not licencees, these forms of enforcement are not available.

In the US, there is a safe harbour provision for hate on the internet. The Communications Decency Act states that:

"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."<sup>21</sup>

This provision goes too far. It is a blanket immunity. There should be a defence of innocent dissemination, but internet provider should be liable for noxious content that is not innocently disseminated.<sup>22</sup>

To able to rely on a defence on innocent dissemination, internet providers should:

- 1) provide a complaints system which generates a response within a reasonable period of time, and
- 2) on notice, remove, or take reasonable steps to remove, hate speech from their services.

As was noted when addressing an internet specific civil remedy, the CBA Sections believe there is value in enacting provisions in the Criminal Code dealing specifically with the internet, even if general provisions arguably provide a remedy. The Criminal Code's hatred offences are offences for communicating hatred, not for advocating for hatred. Internet service providers can be as guilty of these offences as any others engaged in the communication. They should only be liable for communication that is not innocent. It is this sort of liability rather than a variation of Criminal Code provision 320(1) that needs to be enacted.

#### 4. Private conversation

<sup>&</sup>lt;sup>20</sup> Broadcasting Distribution Regulations section 8(1)(b)

<sup>21</sup> Section 230, Communications Decency Act 1996

Peter Leonard, "Safe Harbors in Choppy Waters Building a Sensible Approach to Liability of Internet Intermediaries in Australia" (2010) 3 Journal of International Media and Entertainment Law 221

The Criminal Code prohibitions against incitement to hatred specify three types of communication: communication in a public place, communication in private conversation and communication generally. Communication in a public place objectively amounting to incitement to hatred is prohibited.<sup>23</sup> Communication in private conversation is exempted from liability. Communication which is neither leads to criminal liability only if the communication willfully promotes hatred.<sup>24</sup>

The exemption of private conversation is overbroad. The right to privacy has a foundation in the *Charter*. Privacy interests are an aspect of liberty and security of the person under section seven of the *Charter*.<sup>25</sup> However, the right to privacy should no more trump the right to freedom from incitement to hatred than should the right to freedom of religion. Like all other rights which may clash with the right to freedom from incitement to hatred to be balanced. How they are balanced will depend in the circumstances of the case.

Not all private communications whipping up hate should be immune from the law on the grounds of privacy. In cases where private communication of hate speech may not incite a person who receives the communication, the right to privacy would arguably prevail. In other cases, a private communication of hate speech may incite the recipient to grave acts of violence against people identified by characteristics protected by the legislation.

We recommend removing the exception of private communication from the Code. This removal would not amount to a denial of the right to privacy, which is a right protected by the *Charter* that would have to be considered when applying the Code even if it is not explicitly mentioned. Removing the exception of the right to privacy would allow for balancing privacy rights against the right to freedom from incitement to hatred in the Code.

# IV. OTHER OPTIONS

A. Addressing the gap in data collection and tracking online hate

1. The police

<sup>&</sup>lt;sup>23</sup> Section 319(1)

<sup>&</sup>lt;sup>24</sup> Criminal Code section 319(2)

<sup>&</sup>lt;sup>25</sup> Edmonton Journal v. Alberta (Attorney General), 1989 CanLII 20 (SCC), [1989] 2 SCR 1326 at page 1377

Statistics Canada releases annual reports on police reported hate crimes.<sup>26</sup> Police reporting is often under-reporting because of the police focus on the criminal act instead of the motivation for the act. Deciphering which speech is hate speech requires expertise many police forces do not have. While NGOs engage in incident reporting, hate speech reporting should not be left to them. Police reporting should continue.

While there are questions about the reliability of police reporting due to the tendency to underreport, under-reporting is a vehicle for identifying the absence of police expertise and a means of remedying it. When police know that their hate crimes efforts will be scrutinized and compared with the reports of NGO reports, their efforts to address hate crimes are likely to be enhanced. To remedy the problem, we need to know the extent of the problem.

### 2. The public

Some NGOs run 24-hour hot lines allowing anyone to call and report a hate incident relevant to the mandate of the NGO. NGOs sometimes also have online reporting systems. These reports are a basis for action and an important source of data for public reports.

The Canadian Human Rights Commission does not engage in this type of activity. According to its statute, the Commission is expected to develop and conduct information programs to foster public understanding of the CHRA and its principles, and the Commission's role and activities.<sup>27</sup> This provision encourages one way communication from the Commission to the public.

The CHRA should also encourage communication from the public to the Commission, particularly when it comes to the internet. It takes many eyes to see the high volume of content on the internet. To instill confidence that the Commission is capturing abuse on the internet, there should be an active public education campaign encouraging members of the public to report online hate to the Commission.

## B. Formulating definitions of hate

Definitions of incitement to hatred that are specific to identity groups can help agencies determine what types of expression amount to hate. For example, the International Holocaust Remembrance Alliance has endorsed a definition of antisemitism which the Canadian government and many other member states of the Alliance have adopted. The definition is a

<sup>26</sup> Statistics Canada, <u>Police-reported hate crime in Canada, 2018</u>.

<sup>&</sup>lt;sup>27</sup> Section 27(1)(a)

guideline only and is not binding on law enforcement. The Alliance is currently working on a comparable definition for anti-Roma expression.

Similar definitions should be developed for all forms of hate. It would be useful for the Canadian Human Rights Commission to develop these definitions in consultation with stakeholders. Specific definitions would assist those who do not closely follow the victimization of a group in identifying what amounts to incitement to hatred. The discourse used in stereotyping and incitement to hatred varies depending on the victim group targeted. To identify incitement to hatred, a reader or listener may need to know things which are not obvious in the statement.

Working definitions relevant to each victim group would be helpful in all aspects of anti-hate laws, including the Attorney-General's consent for prosecution.

# C. An international treaty

Much of the internet Canadians access comes from outside Canada. The effort to combat online hate must be a global effort requiring international cooperation.

On July 8, 2005, the Canadian government signed the Council of Europe Additional Protocol to the Convention on Cybercrime.<sup>28</sup> The protocol addresses the criminalization of acts of a racist and xenophobic nature committed through computer systems. Over fifteen years later, the Protocol has yet to be ratified.

The federal government introduced a bill<sup>29</sup> into the House of Commons in 2010 to create the legislative framework necessary for Canada to ratify the Convention and Protocol.<sup>30</sup> The bill never got beyond first reading.<sup>31</sup>

It is long overdue for Canada to ratify this treaty. Canada should generally ratify the treaties it signs. Signing a treaty means that it intends to ratify and comply with the treaty.

<sup>28</sup> Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, 2003.

<sup>&</sup>lt;sup>29</sup> <u>Bill C-51</u>, House of Commons of Canada, 2010

<sup>30</sup> Bill C-51 Bill Narrative/ Descriptor, Parliamentary Budget Officer

Bill C-51, House of Commons of Canada, 2010

Ratifying the treaty would enable Canada to cooperate with other state parties through treatybased mechanisms to realize its goal. After ratifying the treaty, Canada could credibly encourage other states to sign and ratify the treaty and promote the international fight against online hate.

### D. Ongoing consultation

The CBA Sections welcome this consultation and suggest that if the law is changed to allow the Canadian Human Rights Commission and Tribunal to address online hate, there should be consultations on the implementation of the law. The Commission should establish formal consultations with stakeholders on the operation of the law.

Stakeholders' experience with the operation of the law would be a useful resource for the Commission in applying the law. The Commission should be mandated to draw on that experience.

The Commission should be as transparent as possible in dealing with online hate. Regular consultation (e.g. through internet roundtables) would help stakeholders understand any issues, concerns and obstacles that the Commission might face in applying the law.

## V. CONCLUSION

Striking a balance between the right to freedom of expression and the right to freedom from Incitement to hatred and discrimination requires remedies that are not so easy to access as to become vehicles to harass legitimate expression, but accessible enough to be workable.

The previous section 13 of the CHRA went too far in one direction with easy access that led to the harassment of legitimate expression. We recommend reintroducing the substance of section 13 to have a civil tool to combat online hate speech with modifications to avoid the problems that prompted the repeal of this section.

The Criminal Code goes too far in other direction and does not catch enough incitement to hatred. Our recommendations would enhance the effectiveness of this remedy.

It is easy to support respecting a human right where its opposition amounts to a human rights violation. The task is more difficult where respecting one human rights requires balancing against the respect of another human right. With the prevalence and harm of online hate, this task is urgent.

Sectorski, construction to contract of the state of the state of the sector state of the state of the sector of the state of the state of the sector of the state of the state of the sector of the

s.19(1)

## Felicia Mazzarello

From:

Compagnie Théâtre Créole Konpayi Teyat Kreyòl

Sent: To: Subject: July 30, 2021 9:59 AM ICN / DCI (PCH) Lutte contre la haine en ligne

Selon nous au sein de la Compagnie Théâtre créole il faut que les gens soient imputables de leurs réactions en ligne. Il faut que le gouvernement puisse:

- répérer les serveurs quand il y a une réaction négative,

-faire suivre une lettre d'avertissement aux personnes concernées,

-mettre une amende en place et réellement tracer l'exemple,

-il faut cependant faire pour ne pas tomber dans la limite des droits à la parole.

La Compagnie Théâtre Créole reste disponible pour faire partie du débat.

#### Felicia Mazzarello

From: Sent: To: Subject: Igor Williams September 25, 2021 11:58 PM ICN / DCI (PCH) NO to Canada's harmful content proposal

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

s.19(1)

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Igor Williams

Androso, construction construcstra a francisco de artematica Anglia de artematica de artematica Anglia de artematica de artematica Anglia de artematica de artematica

### Steven Wright

From:	Kate Harcourt	s.19(1)	
Sent:	September 2, 2021 8:11 PM		
To:	ICN / DCI (PCH)		
Subject:	Your censorship plan :(		
Categories:	Campaign		

To the Digital Citizen Initiative.

I am responding to your request for written submissions on the proposed approach to online harms. I would like to outline some concerns I have about the proposed approach, which will be ineffective at combating online harm and instead will capture non-criminal content and limit free expression.

I support efforts to remove criminal content from the internet. But the proposed approach will not achieve this goal, and it is unbalanced because it does not reflect concern for the fundamental rights of Canadians.

The proposed 24 hour takedown requirement will lead to platforms proactively removing non-criminal content in order to avoid massive financial penalties. This chilling effect is dangerous to free expression in Canada.

The mandatory police reporting proposal will result in the use of artificial intelligence to proactively monitor Canadian's speech, and AI generated records are likely to include non-criminal speech. I oppose this proposal, which could result in computer generated records of non-criminal speech being proactively sent to police.

The proposal includes three new regulatory bodies, which is an enormous new bureaucratic undertaking. I oppose empowering these bodies to conduct broad inspections, including warrantless inspections of non-regulated businesses. This proposal is too broad, and may violate the right to be free from unreasonable search.

I am concerned by the proposal to allow the Digital Recourse Council to conduct secret hearings. This goes against the open court principle and basic notions of democracy. I am also opposed to the new proposed power that this regulator would have to block websites.

Instead of addressing criminal content, this proposal will drive the content underground to more obscure platforms. I am concerned that the impact of this proposal will be to silence non-criminal expression by everyday Canadians using these platforms.

Please take this plan back to the drawing board.

Yours truly

Kate Harcourt

Sent from Yahoo Mail for iPhone

derazionari economicari e non com no la 20 con Paccha di Varia data con Oberenza di teteri nel tanon con a la concelta teteri nel tanon con a la concelta teteri con con a tro

 From:
 Jack Morrow

 To:
 ICN / DCT (PCH); Steven Guilbeault

 Subject:
 Opposed to Bill C-10

 Date:
 September 25, 2021 9:25:05 PM

Dear Mr. Guilbeault:

This is just a note to declare my opposition to Bill C-10 as an unwarranted and unconstitutional infringement on the rights of Canadians. Please withdraw this bill.

Sincerely,

Jack Morrow

s.19(1)

From:	Ivy Orwell
To:	ICN / DCI (PCH)
Subject:	Have your say: The Government's proposed approach to address harmful content online
Date:	September 25, 2021 12:14:12 AM

I'd like to submit this article as feedback for the proposed approach.

https://techpolicy.press/five-big-problems-with-canadas-proposed-regulatory-framework-forharmful-online-content/

Thanks, Ivy

Get Outlook for Android

Anal Kashi - ann ta sport a cruit (1997) 1945 - China Sark - ar ann taonn 1967 - ann taoin - ann an 1977 1977 - Ann taoin - ann an 1977 1977 - Ann taoin - ann an 1977

 From:
 Liam Whalen

 To:
 ICN / DCI (PCH)

 Subject:
 Digital Citizen Initiative - harmful content online

 Date:
 September 25, 2021 9:23:06 PM

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St Gatineau QC K1A 0S5

To whom it may concern,

Thank you for gathering comments about the proposed changes to police harmful content online. I have not had an opportunity to read much of the details yet. I became aware of this today.

The proposed changes to handling Basic Subscriber Information (BSI) are probably warranted for CSIS. The speed of online communication makes a months long warrant process useless. In the same line of thought, passing BSI information to law enforcement along with reporting may be appropriate.

However, in either case, the reporting of BSI by online communication providers to government agencies should be recorded and retained for as least as long as the data about subscribers will be retained.

In addition, these cases should be reviewed annually to determine the ratio of actionable reporting to reporting that resulted in either no investigation or investigations that led to no criminal proceedings against subscribers. Ideally, these details would be published according to Information Management norms regarding subscriber privacy, so the public can verify if the reporting is effective and not excessive. These reports would help maintain public confidence in these new enforcement powers, which will be characterized as an overreach by some.

Additionally, unacceptable ratios should be defined in the regulation, so the reporting can be adjusted if too much or too little BSI is being reported.

Liam Whalen

s.19(1)

From:	Aaron Klaassen
To:	ICN / DCI (PCH)
Subject:	Comments on "Harmful Online Content" regulatory proposal
Date:	September 25, 2021 3:34:25 PM

I've been working in the tech industry in Canada for nearly two decades in a variety of senior and leadership positions, and am alarmed at this <u>'harmful content' regulatory proposal</u>.

While the objectives of such regulations are no doubt well-intentioned, the devil is truly in the details here: what's being proposed is so vague and far-reaching that it would undoubtedly result in a chilling effect and thus serious restriction of Candians' freedom of expression and privacy. I strongly echo the objections outlined by <u>Daphne Keller at Tech Policy Press</u> and <u>Michael Geist at the University of Ottawa</u>.

As a longtime software developer, I can tell you that the technical requirements for adhering to these regulations would be out of reach for all but the largest organizations, and even then *probably wouldn't even work in the first place* - particularly the "pro-active monitoring." I've spent years working on tech products that accept and scan and categorize user-submitted content and let me assure you that software is not magic; a functioning system as outlined here would be all but impossible in any case: what rate of false positives would be acceptable - how many innocent people will be caught in the crossfire? One would have to be out of their mind to consider establishing a tech startup in Canada under these requirements.

I understand the desire to reduce or eliminate genuinely harmful content; but these tactics - even if they worked, of which I am *extremely* skeptical - will unambiguously do more harm than good.

Aaron Klaassen.

MORINO CONTRACTOR CONTRACTOR ACCONTRACTOR CONTRACTOR MORINO CONTRACTOR CON

s.19(1)

Robert Cox
ICN / DCI (PCH)
Information Overload with Overwhelming Controls
September 25, 2021 2:59:40 PM

Dear Info Consultation,

I must say that

Any government intervention is TOO LATE and just a NEW problem to be added to the complete and utter disaster of human communication on planet Earth. "Credibility" is entirely non-existent for me, and I am sure many feel the same way. The massive amount of internet and other information is similar to the first huge effects of the printing press, but highly magnified.

I started off believing I was free to speak back to certain sites, like CBC internet news making comments available to readers. I am now mostly moderated off of CBC comments, as an Artificial Intelligence moderates certain key words and deletes posts that writers were not aware were triggers for deletion. It's all a mess, I am completely unwelcome at CBC comments.

Yes, that is because I have become "hyper-critical" and NOTHING pleases me. And so, yes, esponses within the acceptable AI parameters of the Moderator. This is a feed-back loop, more info creates more response that is Many

others are "normally" emotionally expressive - like creative artists who create to express their strong emotions. That is what MAKES a person be an artist, there is simply TOO MUCH emotion to ignore, uneasiness results until pressure is released through expression, and sometimes, any one making an "emotionally energized" statement goes beyond the normal bounds.

I now see my ENTIRE "information landscape" a minefield of garbage, stretching inexorably to the horizon of the failing human civilization.

Every single human idea or thought is just rude manipulation attacking my integrity. I am a hopeless addict, but trying hard to turn it all OFF.

I STOPPED watching TV a few years ago, I STOPPED listening to ANY radio more recently. I do NOT have a cellphone since losing one 2 years ago. I do not own a car, I don't have a driver's licence. A poem of mine has a line, "I don't want to see a movie with a gun in it." I was DISGUSTED and angry with the recent election I called a Garbage Election supported by Garbage Media from the first day of the campaign until NOW as I repeat it to you.

I am UTTERLY dismayed and half-destroyed coping with emotional overload during every moment of every day.

The people of a democracy VOTE to elect a government to act on behalf of the population. We don't vote for corporate lobbyists having regular appointments with OUR MPs. We don't vote for MPs to assist corporate rules to command the population. The people don't WANT a government to "regulate" the public - the public wants the government to regulate the corporations. I don't want the Quebec government to regulate my speech. Government regulation must BENEFIT the public, not restrain.

I think he was made crazy by the commemoration of 9/11 and the withdrawal from Afghanistan. He had done two tours of duty in Afghanistan, because he believed in "the war on terror." The end of that "occupation" of Afghanistan in such mediocrity may have prompted just to escape from our ridiculously STUPID humanity which is what I am mourning. The end of the Meng Wanzhou "thing" makes Rule of Law and Government responsibility a stupidity. It is ALL garbage, turn it all off, burn this fucking e-mail, go to hell!!

Robert Cox

s.19(1)

Contrastor - Construction File Contrastor (1997) - Construction File Contrastor (Construction) - Contrastor (1997) - Contrastor (1997) - Contrastor (1997) - Contrastor (1997)

#### Felicia Mazzarello

From: Sent: To: Subject: s.19(1) September 26, 2021 12:55 AM ICN / DCI (PCH) Digital Citizen Initiative -Online Harms Consultation

I am writing on behalf of <u>Parents Aware</u> to provide some comments regarding the proposed framework in dealing with online harms. As Parents Aware's main focus is helping parents have conversations with their children surrounding the harms of pornography, I will be commenting on 2 of the online harms: CSAM and the non-consensual sharing of intimate images.

Since the development of the internet, the pornography industry has exploded. With the millions of videos available and uploaded to websites and social media platforms it is almost impossible to monitor and police this industry. Companies, websites and social media platforms that host pornographic material should be required to take proactive measures to prevent uploading CSAM and intimate images shared without consent. All individuals depicted in the videos/images should have their age verified and have given written consent prior to any filming or uploading of material to websites or social media. Any sites that host this material should comply with the regulatory demands and if they do not, should be held criminally responsible for all offenses.

I feel that the proposed changes to strengthen the Mandatory Reporting Act should be adopted. I feel that implementing option #2 would provide law enforcement the information needed to locate offenders and rescue victimized children faster.

The type of pornography created and viewed today is violent, degrading, dehumanizing, racist and full of hate speech. Unfortunately it is shaping the fabric of society to treat women as sex objects where violence is normal. Pornography is also rampant with CSAM. The devastating social impact on individuals, children, families and our community is very apparent.

We are pleased that the government is addressing online harms in an effort to make the internet safer, protect the vulnerable and empower those who are victimized.



Lisa Whitsitt Director of Educational Outreach, Parents Aware

www.parentsaware.info

AnnM
ICN / DCI (PCH)
The Government's proposed approach to address harmful content online
September 25, 2021 10:43:08 PM

Why is it that the governement feels the need to censor people on social media, or any the media for that matter?

This is obviously wrong and there is no reason to push for a chinese communist party type society for Canada.

We are supposed to be a democracy, and we still have a bill of rights, and it should be followed, free speech and freedom of expression is part of that. The freedom of expression in the Charter is there to stop the government from stopping us from expressing ourselves.

What will be termed hate speech? There are already laws concerning hate speech and racsim, which are followed.

There is already way too much censorship in the media, as many outlets were paid by government. Done without any input of the taxpayers who unkowingly have given way too much mony to the media outlets who continually suppress free speech in favour of constant propaganda to promote vaccines and unlawful lockdowns and other "health measures" to promote an untested "vaccine" not approved by the FDA with no consequenses or liability to the pharmaceutical companies who already have a track record of harming people with their drugs.

On April 30, 2021, Ontario's physician licensing body, the College of Physicians and Surgeons of Ontario (CPSO), issued a statement forbidding physicians from questioning or debating any or all of the official measures imposed in response to COVID-19. That is stifling free speech right there. Its dangerous to all of us.

So you see the censorship is already bad enough without also going after social media too. The legislation seems vague. What would be considered terrorist content or content that incites violence or just hate speech..? who will be deciding?

Obviously most people do not condone real hate speech and especially exploitation of children.

I am appalled at what has been going on in Canada under the guise of health.

Please dont help this unlawful very corrupt government continue on this road, so far thier actions have shown me they are not to be trusted, for example Imposing a vaccine passport going against the basic human right of autonomy over one's own body.

I hope the public input will matter. Sincerley

Ann McIvor s.19(1)

derzenista estatuta aporte a contra pota 201 entre a contra de la contra contra a Obra consol de estatuta contra da la la estatuta de la contra contra da la contra la estatuta da la contra contra da la contra la estatuta da la contra d

 From:
 Maurice LaBrie

 To:
 ICN / DCI (PCH)

 Subject:
 Legislating online content

 Date:
 September 25, 2021 10:58:33 PM

The legislation you propose is a gross overreach into the private communications of Canadian citizens. I am deeply offended that you could even consider this as being prudent moral behavior. How dare you.

Maurice LaBrie

s.19(1)

Sent from Mail for Windows

#### Commentaires et suggestions formulés dans le cadre de la consultation publique concernant l'approche proposée par Patrimoine Canada pour règlementer les réseaux sociaux en juillet 2021

#### Observations

L'approche proposée vise à traiter les messages « préjudiciables » publiés sur les réseaux sociaux.

Elle oblige les plateformes à investir temps et argent pour identifier évaluer l'ensemble des messages et supprimer les messages problématiques.

Cette approche ne s'attaque pas à la source du problème. Elle laisse le problème se produire.

Serait-il possible d'adopter une approche qui s'attaque à la source du problème, avant même qu'il ne se produise? Si oui, une telle approche serait moins couteuse et moins dommageable.

#### Suggestions

Voici trois suggestions qui permettraient de limiter grandement la production et la publication des messages « préjudiciables. Ces suggestions peuvent être considérées comme complémentaires à l'approche proposée par Patrimoine Canada.

- Rendre obligatoire la publication du nom des personnes qui écrivent des messages sur les réseaux sociaux.
- Mettre en place un timbre, une taxe ou un «ticket modérateur» payable par la personne qui publie un message sur les réseaux sociaux.
- Mettre en place un code de « cohésion sociale » prévoyant des infractions et des amendes pour la publication de messages haineux.

La 1ere mesure a été évoquée par le codirecteur de <u>l'Observatoire sur la radicalisation et l'extrêmisme violent</u>, M. David Morin, lors d'une entrevue diffusée à l'émission 24/60, le 31 janvier 2020.

La 2<sup>e</sup> mesure s'inspire du système postal. Tout le monde peut recevoir du courrier gratuitement. Mais on doit payer un timbre pour faire un envoi à un ou plusieurs destinataires. Plus le nombre de destinataires est grand, plus ça coûte cher à l'émetteur. Si un message franchit une frontière, le prix du timbre est plus élevé. Ainsi, pour publier un message sur un réseau social comptant des milliers de membres, le prix des timbres serait dissuasif pour les émetteurs de messages « préjudiciables ».

La 3<sup>e</sup> mesure est une prolongation de la charte des valeurs et pourrait être calquée sur le code de la sécurité routière.

Sachant que les fournisseurs de services téléphoniques et d'accès à internet sont capables de facturer les communications à la seconde près, on peut estimer que ces mesures sont réalisables sur le plan technique.

Sachant que les fournisseurs de services téléphoniques et d'accès à internet disposent déjà d'un système de facturation de leurs clients, le gouvernement pourrait les mandater pour collecter les montants reliés aux timbres et aux amendes.

Sachant que les messages préjudiciables, publiés sur les réseaux sociaux sont une plaie pour la société et qu'ils font des victimes partout dans le monde, les gouvernements auraient avantage à se concerter pour mettre en place de telles mesures sur leur territoire respectif.

**Bernard Frigon** 

s.19(1)

Machanya and Actina and Actina

#### Felicia Mazzarello

From: Sent: To: Subject: Michelle L. < July 29, 2021 4:41 PM ICN / DCI (PCH) Digital Initiative

s.19(1)

Categories:

Steven

Wow, what a great idea! A true win for democracy for sure, along with workplace training such as employee mental illness day because it must be employees not grasping the full head on support provided by mangers, that's right in front of their eyes, and your way of SUPPORTING actual good and honest workers in the public service, that has been loyal to her majesty and the system and herself. As a former public servant that contracted the virus during the misfortune of having been framed for something she did not associate with her moral character, miraculously recovered and be treated with such a great warm former work environment to continue the narrative, I had to bid them farewell because it was just such a fantastic management team.

I now happily look towards a brighter future to serve my fellow people & country that respect me, with only good references from my former workplace because of my truly consistent superior work ethics and kindness I provided during my tenure, to move on to better genuinely supportive work environments. Perhaps my mindset and so perceived mental health shall be better once the problem is resolved.

All the Best,

Michelle Ly

Socialisti contra que constituen este a francesión de ataliante Socialista constituente de Socialista constituente de Socialista constituente

From:	Rita Brooks
To:	ICN / DCI (PCH)
Subject:	Government's proposed approach to address harmful content online
Date:	September 24, 2021 7:28:39 PM

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St Gatineau QC [K1A 0S5]

To whom it may concern,

After going through the Discussion Guide and Technical Paper I see a huge problem with the Canadian government's proposed recommendations for legislation to address "harmful online content".

It appears rather that the government is less interested in addressing harmful online content than it is in gutting the current due processes that are in place for law enforcement, as well as suspending corporate liability and accountability.

For instance, considering only two (2) of your recommendations I see huge problems:

Section 31 under Module 1(B): New rules and obligations:

"The Act should provide that OCSPs [online communication service providers] making (a) notifications to the RCMP or (b) reports to law enforcement and CSIS in good faith pursuant to the Act should have immunity from civil and criminal proceedings."

These proposals recommend handing unrestricted power to unaccountable online platforms to surveil, police and remove content. Where is the accountability?

And Section 3 under Module 2: Modifying Canada's existing legal framework re: Canadian Security Intelligence Service Act (CSIS)

"The Act should provide for a more expedient process to ensure timely investigations and greater flexibility than the section 21 regime currently provides, particularly by simplifying the procedures as compared to section 21."

So no due diligence?? No oversight?? Is the government proposing that Section 21 of the CSIS act be sidelined because it finds "having reasonable grounds" for a warrant onerous?

Currently restrictions on our freedom of speech are properly limited, and surveillance by law enforcement requires that the most basic due diligence is completed in order to get approval of a court. Why on earth would the Canadian government and its agents want to eliminate this most basic safeguard?

**Rita Brooks** 

Mona Piece	
ICN / DCI (PCH)	
Online Harms - proposing new regulations - likely will cause harm	
September 24, 2021 10:34:03 PM	

The proposed framework, though some will argue is well-intentioned - ie ensuring companies like Google do better in addressing harmful content and behavior online - would have harmful consequences on human rights.

Specifically it would create new regulations for "harmful content" potentially including lawful speech, in ways that can be misused for censorship and surveillance.

It includes a wide ranging framework to regulate Online Harms, proposing new regulations to govern user activity online with a myriad of new regulatory agencies to enforce them.

The framework includes some of the most problematic proposals, includ:

- proactive monitoring of content
- 24 hour removal time (or face substantial financial penalties
- mandatory offramp to law enforcement
- access to user information, along with a gag order
- data retention requirements
- potential for isp blocking by a regulator
- pursuit of information related to software algorithms

Just a thought - We would expect this from an entirely different political party. And we don't vote for them.

Standards - construction to the contract of the the contract of the contrac

#### Felicia Mazzarello

From:	Andree-Anne PERRON <andree-anne.perron@montreal.ca></andree-anne.perron@montreal.ca>	
Sent:	July 30, 2021 1:06 PM	
To:	ICN / DCI (PCH)	
Subject:	Consultation pour un environnement numérique plus sur - contre la haine en ligne	
Follow Up Flag:	Follow up	
Flag Status:	Completed	
Categories:	FR	

#### Bonjour,

J'ai consulté les différents documents disponibles, peut-être que l'information m'a échappé, auriez-vous l'amabilité de me préciser la date limite pour déposer un écrit dans le cadre de cette consultation s.v.p.? Je comprends qu'un projet de loi serait déposé à l'automne. Avez-vous une idée précise du moment? De plus, pourriez-vous me préciser s'il s'agira du seul mode de consultation ou si des rencontres avec des partenaires/experts/groupes sont également prévues?

Merci beaucoup Bonne journée

Andrée-Anne Perron Conseillère Bureau des relations gouvernementales et municipales Ville de Montréal

Hôtel de ville - Édifice Lucien-Saulnier 155, rue Notre-Dame Est Annexe - Local R-100 Montréal (Québec) h2Y 1B5 <u>andree-anne.perron@montreal.ca</u> Téléphone cellulaire: 438 354-4127

\*Actuellement en télétravail\*

**AVERTISSEMENT** : Ce courriel et les pièces qui y sont jointes sont destinés exclusivement au(x) destinataire(s) mentionné(s) ci-dessus et peuvent contenir de l'information privilégiée ou confidentielle. Si vous avez reçu ce courriel par erreur, ou s'il ne vous est pas destiné, veuillez le mentionner immédiatement à l'expéditeur et effacer ce courriel ainsi que les pièces jointes, le cas échéant. La copie ou la redistribution non autorisée de ce courriel peut être illégale. Le contenu de ce courriel ne peut être interprété qu'en conformité avec les lois et règlements qui régissent les pouvoirs des diverses instances décisionnelles compétentes de la Ville de Montréal.

 From:
 Justin Elchel

 To:
 ICN / DCI (PCH)

 Subject:
 Please do not inplement the proposed censorship plan

 Date:
 September 24, 2021 9:01:16 PM

Hello,

I'm writing to express my concern over the proposed censorship plan. I do NOT support a dragnet approach to internet censorship. Both the RCMP and CSIS have a history of monitoring and harassing minority groups, 2SLGBTQ+, first nations, black, people of Asian decent, and women to name a few. They should NOT be the ones in position of power in this relationship. People need to have freedom to express themselves and not have to fear further harassment from CSIS and RCMP. If this goes forward you need a new neutral and impartial agency. As written it is not a good position for Canadians.

Thank you, Justin

From:	Ben Poole
To:	ICN / DCI (PCH)
Subject:	Comment on Proposed Legislative & Regulatory Framework for Addressing Online Harms
Date:	September 24, 2021 8:00:59 PM
Attachments:	POOLE-OnlineHarmsComment.pdf

Attention: Digital Citizen Initiative,

I have attached my comments concerning the proposed legislative and regulatory framework for addressing online harms.

Regards, Benjamin Poole

From:	David Rattray
To:	ICN / DCI (PCH)
Subject:	Proposed approach for harmful content online
Date:	September 23, 2021 11:45:16 AM

#### Hello,

I'm deeply concerned about the strong potential for government overreach with the new proposal. While I agree that there are many things on the internet that are unsavory or dangerous, I am not in favour of increasing the scope of surveillance that Canadians are under, nor outsourcing the surveillance to private companies. I think the RCMP and CSIS need to work on improving the eroded trust after the revelations about their surveillance of environmental activists and others who were never a threat to any Canadian citizen.

We do not need a NSA Prism program in Canada, and I doubt we ever will. This proposal needs to be scrapped.

David Rattray

PhD Candidate Foster Lab Networks of Centres of Excellence, UBC.

s.19(1)

# Rebuilding Canada's Public Square

Response to Government of Canada's Proposed Approach to Address Harmful Content Online

September 2021

Sam Andrey | Alexander Rand | M.J. Masoodi | Karim Bardeesy

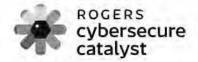


Dissumment commonly in our annum la Esti aux rannos à l'information Disconsent mississit aux qui et la Dis Access la consumment dell



#### Cybersecure Policy Exchange

The Cybersecure Policy Exchange (CPX) is an initiative dedicated to advancing effective and innovative public policy in cybersecurity and digital privacy, powered by RBC through Rogers Cybersecure Catalyst and the Ryerson Leadership Lab. Our goal is to broaden and deepen the debate and discussion of cybersecurity and digital privacy policy in Canada, and to create and advance innovative policy responses, from idea generation to implementation. This initiative is sponsored by the Royal Bank of Canada; we are committed to publishing independent and objective findings and ensuring transparency by declaring the sponsors of our work.



#### Rogers Cybersecure Catalyst

Rogers Cybersecure Catalyst is Ryerson University's national centre for innovation and collaboration in cybersecurity. The Catalyst works closely with the private and public sectors and academic institutions to help Canadians and Canadian businesses tackle the challenges and seize the opportunities of cybersecurity. Based in Brampton, the Catalyst delivers training; commercial acceleration programming; support for applied R&D; and public education and policy development, all in cybersecurity.



#### Ryerson Leadership Lab

The Ryerson Leadership Lab is an action-oriented think tank at Ryerson University dedicated to developing new leaders and solutions to today's most pressing civic challenges. Through public policy activation and leadership development, the Leadership Lab's mission is to build a new generation of skilled and adaptive leaders committed to a more trustworthy, inclusive society.

Dissument commonly in version In Emilian and annota in Parlamentari Darianent released and annot to The Access Reconstruction in t

#### How to Cite this Report

Andrey, S., Rand, A., Masoodi, M.J., and Bardeesy, K. (2021, September). *Rebuilding Canada's Public Square*. Retrieved from https://www.cybersecurepolicy.ca/public-square.

© 2021, Ryerson University 350 Victoria St, Toronto, ON M5B 2K3



This work is licensed under a <u>Creative Commons Attribution-NonCommercial-ShareAlike 4.0</u> International License. You are free to share, copy and redistribute this material provided you: give appropriate credit; do not use the material for commercial purposes; do not apply legal terms or technological measures that legally restrict others from doing anything the license permits; and if you remix, transform, or build upon the material, you must distribute your contributions under the same licence, indicate if changes were made, and not suggest the licensor endorses you or your use.

#### Contributors

Nour Abdelaal, Policy Analyst, Cybersecure Policy Exchange Sam Andrey, Director of Policy & Research, Ryerson Leadership Lab Karim Bardeesy, Executive Director, Ryerson Leadership Lab Sumit Bhatia, Director of Innovation and Policy, Rogers Cybersecure Catalyst Zaynab Choudhry, Design Lead Charles Finlay, Executive Director, Rogers Cybersecure Catalyst Mohammed (Joe) Masoodi, Senior Policy Analyst, Cybersecure Policy Exchange Alexander Rand, Research and Policy Assistant, Cybersecure Policy Exchange Stephanie Tran, Research and Policy Assistant, Cybersecure Policy Exchange Yuan Stevens, Policy Lead, Cybersecure Policy Exchange

For more information, visit: https://www.cybetsecurepallcy.cd/



G staybernalicys

in Cyberseoure Policy Exchange

Document communiqué en vertu o la Loi sur l'acces à l'Information Document released pursuant lo Me Access lo information Act

# Executive Summary

Social media is in many ways the new public square — where most Canadians now connect with friends and family, and engage in civic discourse. It has increasingly become clear that this new square is having a foxic influence on our society and democracy, hate speech and harassment targeting marginalized people, disinformation enabling extremism and conspiracy theories to flourish; and online activities fueling real-world violence and exploitation.

Over the past three years, we conducted national representative surveys with Ganadian residents on these important issues. Key findings include:

- More than one in three Canadian residents report encountering harmful content online at least weekly, such as hate speech and violent material
- That figure rises to about halt of those who regularly use social media tor news and current events.
- Racialized Canadians are 50% more likely than non-racialized Canadians to encounter racist content online and report content to platforms for being hateful
- Canadians do not trust social media platforms to act in the public's best interest. In fact, they are less trusted than oil campanies: telecommunication providers and news media.
- 71% of Canadians want the government to intervene in social media companies in 2021 — up from 61% in 2019.
- 75% of Canadians support requirements for platforms to delete illegal content in a timely manner such as hate speech harassment and incidement to violence

Rebuilding Ganadale Public Square: Response to Government of Ganadals Proposed Approach to Address Hormfül Content These results underscore that Canadians are concerned about what they experience on social media and are looking for action to help address the horms produced. The unique reach and speed of social media platforms call for unique regulatory solutions aimed at countering the spread of online harms, while at the same time protecting Canadians rights and freedoms, including our right to free expression. The Government of Canada has **announced its intention** to introduce new legislation to address some of these harms, namely, hate speech; terrorist and violent content; child sexual exploitation; and non-consensual sharing of intimate images.

Decliment communique en viertu e la Lor sur l'acces a l'information Discument released pursvant lo Me Access to microsofton Acc

# Intent of Report

This report is intended to provide our best advice on how to begin genuinely rebuilding this new public square in a manner that protects and advances Canadians' fundamental rights and freedoms and furthers efforts at international platform governance alongside allied jurisdictions. Our recommendations to improve the Government's proposal include:

- Clarity the online platforms in scope to exclude journalism platforms and platforms where user communication is a minor ancillary leature of a platform (e.g., fitness, shopping, trovel)
- Establish platform size thresholds to place fewer obligations on smaller and non-profit platforms to avoid entrenching incumbents
- Require minimum standards of user reporting features and transparency for private platforms with very large user reach.
- Clarify the definitions of harmful content as it relates to online content moderation and consider adding identity fraud to list of harmful content in scope
- Narrow the requirement for platforms to take "all reasonable measures" to identify harmful content to avoid over-cerisorship and ensure wrongful takedown is appealable

- Ensure the length of time provided for content moderation decisions can evolve through regulatory changes
- 7. Limit any requirements for mandatory platform reporting to law enforcement to cases where imminent risk of serious harm is reasonably suspected and consider narrowing to only child sexual exploitation and tenorist content
- Ensure platform transparency requirements are publicly accessible in a manner that respects individual privacy and work with international allies to ensure data comparability
- Require larger platforms to cooperate with independent researchers and annually review and mitigate their systemic risks
- Remove or significantly narrow the ability to block access to platforms for noncompliance



# Introduction

Social media is increasingly used by Canadians to stay up-to-date with the news, connect with friends and family, and engage in civic and political discourse. It is no wonder that many have referred to social media as our new public square. But over the past decade, it has become increasingly clear that this public square is also responsible for producing negative effects on society: hate speech and harassment that target racialized communities and other marginalized groups are rampant; disinformation is abound while helping extremist content and conspiracy theories to flourish: and real-world violence including sexual abuse and child exploitation is unfortunately an increasing reality."

The impacts of this digital transformation on Canada's communications ecosystem are continuing to take shape and are still not fully understood. Indeed, new and emerging platforms continue to develop and rise, often blending public and private communication in ever-changing ways, creating a dynamic ecosystem. However, what is becoming clear at this moment is that the spread of online harms through social media is real and poses significant risks to Canada's social cohesion, public safety and democracy. As a result, there have been growing calls for technical and regulatory changes to mitigate these harms and rebuild our "public square." <sup>bit in the</sup> At the same time, legitimate concerns have been raised regarding over-censorship of online content and that any changes may unreasonably limit our rights and freedoms, particularly the right to free expression."

The Government of Canada has laid out in commendable detail what its intentions are with respect to addressing some of these online harms. The goal of this report is to respond to the Government's proposed approach to address harmful content online, and share the results of representative surveys that we conducted in Canada over the course of the last three years on these important questions.

We believe the results of regular surveys such as these, while imperfect, are important tools as we know so little about these platforms, in part because of the lack of meaningful transparency, cooperation with independent research, and regulatory action to date. Any action in this area should be informed by evidence about Canadians' experience with those harms, as well as Canadians' views on the appropriate role of government in addressing those harms. This report is intended to reflect and provide our best advice on how to do so in a manner that protects and advances Canadians' fundamental rights and freedoms.

la Leo anc Panada à 100 formalion. Document released overvant in The Access to othermanist - 21

# Canadians' Experience on Social Media Platforms

Three national representative surveys conducted by our team over the course of three years (2019, 2020 and 2021) provide a comprehensive picture of the social media landscape in Canada. We provide a summary here as we believe a clear understanding of the significant and growing role of social media in Canada is foundational to designing solutions to the online harms facilitated through those platforms.

# **Overall Use of Platforms**

Most Canadians are using social media platforms — many every day (Figure 1). In fact, more than half of Canadians aged 18-29 report using YouTube (65%), Instagram (52%) and Facebook (51%) at least every day.

Canadians are also increasinaly using private messaging apps to connect and share content. More than 8 in 10 report using private messaging apps in 2021, with Facebook Messenger, WhatsApp and Instagram direct messages as the most used platforms (Figure 2). As with public platforms, there were significant differences in the use of platforms across age groups: the majority of those aged 16-29 used direct messaging on Instagram (72%) and Snapchat (65%), compared to 15% and 8% respectively among those aged 45 and older.

		THE MEETERS TO OTTOM STOC	
		OVERALL / DAILY	
	YouTube	91% / 44%	
	Facebook	75% / 38%	
	Pinterest	51% / 14%	
	Instagram	48% / 27%	
	Twitter	44% / 19%	
	LinkedIn	40% / 10%	
	Reddit	32% / 11%	

n=3.000

Figure 1: Canadians' Use of Social Media Platforms Overall and Daily (2019)

83%	Any Messaging App
72%	Facebook Messenger
35%	WhatsApp
33%	Instagram DMs
24%	Snapchat
13%	Twitter DMs
10%	Discord
33% 24% 13%	Instagram DMs Snapchat Twitter DMs

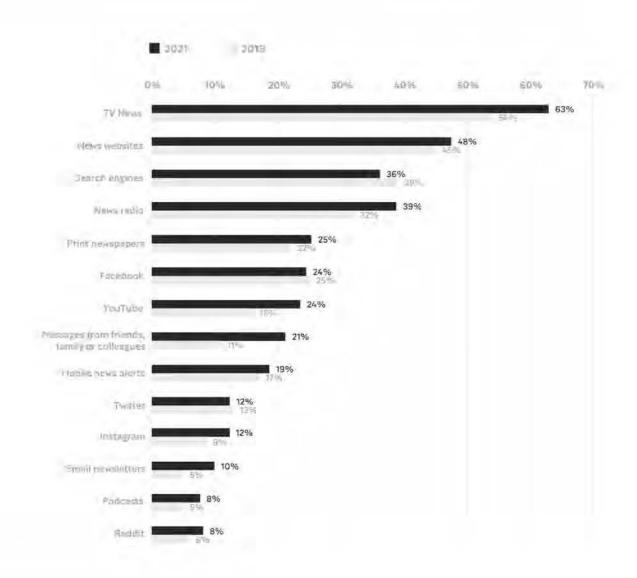
n=2.451

Figure 2: Canadians' Use of Private Messaging Apps Overall (2021)

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content

## Platforms as a News Source

While traditional media, such as television, radio and newspapers, continue to play large roles in how Canadians consume news, one in four Canadian residents report using Facebook and YouTube to stay up-to-date with the news and current events, with 21% using messages from friends, family and colleagues (**Figure 3**). Differences by age are again significant — those aged 16-29 use YouTube (43%), Facebook (35%), Instagram (35%) and private messaging (35%) for news at greater or comparable rates than news websites (42%) or traditional media such as TV (42%) and radio (23%)(**Figure 4**).



#### n=2,451 (2021); 3,000 (2019)

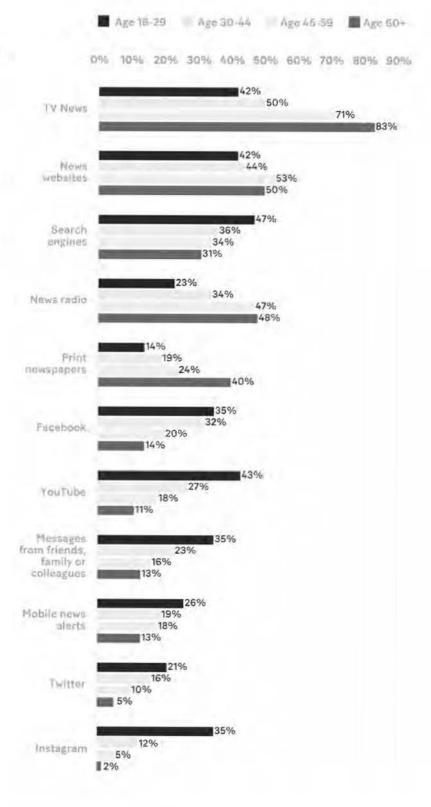
Figure 3: Canadians' Reported Sources for News and Current Events

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content

8

Occument communicati en vient de la En aux hende à l'information Document released, pursivent lo line Access In Minimation Acs

In addition to consuming news, a significant proportion of Canadian residents actively engage with news and politics on these platforms. According to our 2019 survey, 43% of respondents 'like' a news or political post or story on social media at least once per week, 40% join social media groups about an issue or cause, 33% share news/ political stories on social media at least weekly and 30% comment on a news/political post in their own words at least weekly.



#### n=436 (16-29); 636 (30-44); 654 (45-59); 725 (60+)

Figure 4: Canadians' Reported News Sources by Age Group (2021)

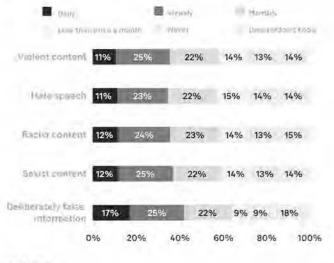
Giocommit commonispli en Arridon la Esu auc casado à l'Information Distanemit mileacest company fis disc Access Rominamanistri Act

# **Exposure to Online Harms**

Amidst this increasing use of social media platforms is a significant degree of reported exposure to harmful content.

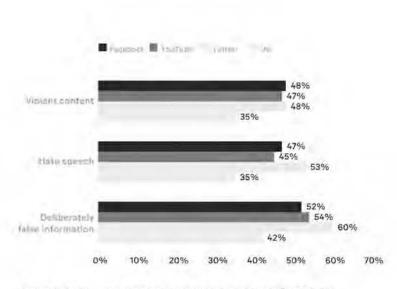
In our 2019 survey, 42% of Canadian residents report seeing deliberately false information on online news sources, including social media platforms, at least once per week (**Figure 5**). More than one third of respondents reported encountering other types of harmful content at least once per week including sexist content, racist content, hate speech, and violent content, with nearly 60% reporting seeing at least monthly.

Further, those that used Facebook, Twitter and YouTube to stay up-to-date on news and current events were significantly more likely to report encountering online harms at least weekly (**Figure 6**).



n=3,000





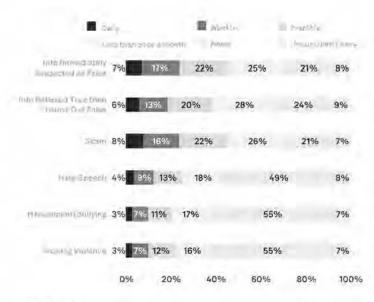
n=754 (Facebook); 490 (YouTube); 405 (Twitter); 3,000 (all)

Figure 6: Canadians' Using Social Media for News Report More Frequent Exposure to Online Harms (2019)

Dissument commonique on versitor la Lin que hanaés à l'Ottornation Do current méssent porquant to the Access la minimulian dei

In our 2021 survey, we asked respondents how frequently they encountered a range of online

harms specifically through private messaging apps. About half (46%) reported seeing information that they immediately suspected was false at least a few times a month; while 39% reported seeing information that they initially believed was true, but later found was at least partially false, with the same frequency. Scam or phishing messages were also reported as a relatively frequent occurrence, with 46% reporting receiving these messages at least a few times a month. Hate speech was identified by 26% of respondents at least a few times a month, with 22% encountering content that promoted or encouraged violence and harassment or bullying at least a few times a month.



n=2.044

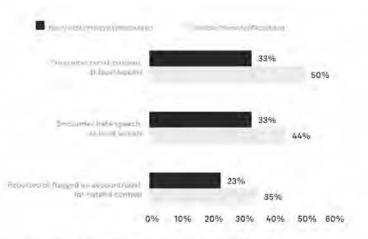
Figure 7: Canadians' Reported Exposure to Online Harms through Private Messaging Apps (2021)

Respondents who used private messaging apps as a regular news source were also more likely to believe a number of common false conspiracy theories about COVID-19 (see Private Messaging, Public Harms for more information). 63% of believers in COVID-19 conspiracy theories received news through Facebook Messenger at least a few times a week, compared to an overall average of 47%. In turn, compared to the average Canadian, COVID-19 conspiracy believers are 34% more likely to get their news regularly from Facebook Messenger. Similarly, 39% of believers in COVID-19 conspiracy theories received news through WhatsApp at least a few times per week, compared to 22% overall, making them 77% more likely to receive their news in this way. This echoes the findings from previous research that found a correlation between consuming news on social media platforms and the likelihood to believe in COVID-19 conspiracy theories.

Racialized respondents also report more frequent exposure to online harms on public and private platforms. Our 2019 data showed that those who identified as racialized were 33% more likely to report encountering hate speech and 52% more likely to report encountering racist content at least weekly, compared to non-racialized Canadians. In our 2021 survey, hate speech was reportedly received through private messaging apps by about one-quarter (26%) of respondents at least a few times a month. However, reported rates were significantly higher among Latin American (58%), Middle Eastern (44%), Southeast Asian (44%) and Black (40%) respondents. These findings strongly indicate that exposure to online harms on social media platforms are experienced more by marginalized communities.

Glassammi commonique on verdes la Lav aux hanaés à l'Alformation Do consent velossent document ro De laceas la entremener dei

One in four respondents in 2019 had reported harmful or fake posts or accounts. Again, those who identified as racialized were also 52% more likely to report an account or post for hateful content (35% of racialized individuals compared to 23% of non-racialized). Likewise, 22% of respondents in 2021 reported someone for sending illegal, hateful or harassing content on a messaging app, with rates significantly higher among people of colour. Of those that did make reports about hateful content on social media, 38% ranked its effectiveness (from 1 to 9) as 7-9, 39% ranked 4-6 and 23% ranked as 1-3. These numbers were very similar for private messaging apps: when asked a similar question in 2021, 35% gave 7-9, 39% ranked 4-6 and 21% said 1-3. These assessments indicate that harmful content reporting to platforms can be an effective mechanism to mitigate harms.



n=2,450 (not); 540 (visible minority/racialized)

Figure 8: Racialized Canadians Report Online Harms More Frequently (2019)

Geoammit communique en virmu de la Lai aux Parisés à Philominkon Document intersett pursuent to the Access to Minimation Act

# Canadians' Views on Platform Regulation

# Low Trust in Platforms

A consistent finding across all three surveys is that **Canadian residents do not trust social media platforms.** Specifically, Canadians do not believe that these companies, including Facebook, TikTok, Twitter and Instagram, make decisions in accordance with the best interest of the public. When asked to rate how much they trust various organizations on a scale

Lie Les 24 Dethion

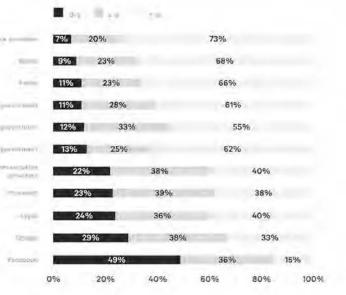
6% 26% NAME OF COLUMN 62% 5% 9% 32% 55% 4% 9% 29% 6% La PSmith 55% 9% 37% 49% 5% 10% 27% 59% 3% 1-10% 37% 48% 5% Historiatt 10% 36% 47% 6% German Served. 119% 34% 49% 6% 680 11% 37% 42% 10% Constant 12% 37% 16% hond introl 36% 39% 12% 35% 15% J Proj 41% 6% 12% BART BAR 41% 13% 30% 50% 7% 1.000 13% 38% 19% 30% Treamin Star 31% 6% TWO 14.9% 49% 35% 43% 8% WALCON! 38% Castin.) 15% 36% 10% 18% 40% South Classics 34% 7% 20% 34% 23% 23% in committed (2011) 34% 21% 21% WINIAM 38% 23% 13% 31% 35% 21% 13% Tutter 18% 36% 30% 16% 39% 3% 21% 37% 0% 20% 40% 60% 80% 100%

#### n=2,451

Figure 9: Canadians' Trust to Act in Public's Best Interest (on a scale from 1-9) (2021)

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content from 1 to 9, respondents were less trusting of social media platforms than oil companies, telecommunication providers and news media (**Figure 9**). Our surveys found that trust in Facebook, including the other services and apps it owns, declines moderately with age, particularly among men.

We also found that big tech companies are less trusted than governments and other public and private institutions to keep personal data secure (**Figure 10**).



#### n=2,000

Figure 10: Canadians' Trust to Keep Personal Data Secure (on a scale from 0-10)(2020)

The consistent low level of public trust in social media companies among Canadians, despite the turbulent years that filled the gap between these two surveys, contributes to the overall impression indicated by the data that Canadians have a strong appetite for greater intervention.

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content Document communique en verte e le Loi sur l'acces a l'informetion Document released pursuant to the Access to information Act

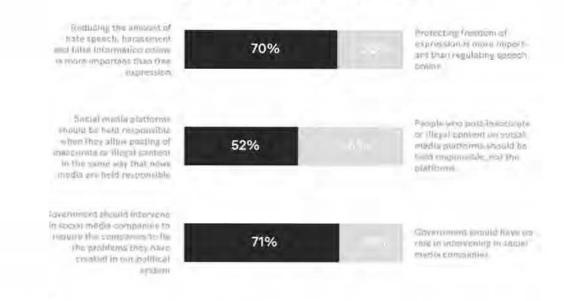
Observant commonly at an army of to the size factors a to formetion Do correctly where the or over to the Access to momentarian det

# A Role for Government

Survey results from both 2019 and 2021 indicate that most Canadian residents are prepared for government intervention to address online harms. When asked in 2019, 80% of Canadians said that an increase in false information spread deliberately was a problem affecting Canadians and society in general, while 70% of Canadians said they thought the role social media plays in our political system was a similar problem.

We asked Canadian residents to choose among a series of statements which best described their perspective, and each indicated a growing willingness for platform intervention. In 2019, 63% of respondents said that reducing the amount of hate speech, harassment, and false information online was more important than protecting freedom of expression. When asked again in 2021, this number had increased to 70% (**Figure 11**). There was also a small increase in the proportion of respondents who believe that social media platforms should be held responsible when they allow posting of illegal or inaccurate content in the same way that traditional news media are held responsible, from 47% to 52%. Most strikingly, the percentage of people who said that the government should intervene to require social media companies to fix the problems they have created in our political system increased from 60% to 71% between the two surveys.

While Canadians' desire to see government action on this issue appears to have increased between 2019 and 2021, their opinions with respect to specific policy interventions — such as requiring platforms to delete harmful content in a timely manner or delete the accounts of users intentionally spreading false information — have remained stable during the same time period.



0% 20% 40% 60% 80% 100%

#### n=2,122; 2,162; 2,018

Figure 11: Canadians' Views on the Role of Government Regulation (2021)

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content

Desamini commonique en vinui de la Lev que l'anaés à l'information De turrent vileo sett pursuont le De lucedor la minimation des

One key takeaway from Canadians' opinions around specific policy interventions is that the policies that were most supported by Canadians were those that imposed new responsibilities for content moderation on the platforms themselves, with opposition to these policies never exceeding 10% of respondents (Figure 12). Policies that would address these issues in an indirect way — such as by funding digital literacy programs for Canadians or by supporting traditional media outlets as an alternative to social media — had generally lower levels of support across both surveys.

Another key point is that while Canadians are generally supportive of various approaches that place responsibilities on platforms to moderate the content that they host, that support diminishes when the approach would result in significant changes to the service being provided. For example, when asked in 2021, 45% of respondents were less supportive of imposing new responsibilities on Facebook if those measures would cause Facebook to shut down operations in Canada, and 54% were less supportive if it would require Facebook to charge a \$5 monthly fee to users (their approximate revenue per user). However, there was more willingness to impose content moderation responsibilities if it would result in Facebook needing to delay posts by a few minutes in order to carry out content moderation - only 18% of Canadians were less supportive in this case, whereas 43% were more supportive.



#### n=2,451

Figure 12: Canadians' Support for Policy Interventions (2021)

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content

Somewhat surprisingly, the survey data did not indicate any strong relationship between trust in social media companies to act in the public's best interests and support for more stringent requirements for those companies. This is in part explained by the broad levels of support for greater action, where even those with high trust in social media companies are still supportive of intervention. Less surprisingly, those who report being victims of various online harms, such as privacy breaches and account hacks, have significantly greater support for intervention than those who have not been victims.

We believe these results collectively paint a clear picture: Canadians are ready for new action to address online harms while maintaining access to services that enable them to connect and share with others. It is worth noting that when Canadians were asked who they trusted the most to address the issue of disinformation, hateful speech and extreme views on social media, no clear consensus emerged. 28% indicated trust in the handling of the issue by social media platforms themselves; 22% by a government agency; 19% by the people who use social media; and 23% were not sure. We believe a takeaway from this could be that while Canadians are prepared for action, they are not sure who is best positioned to lead this work. We believe approaches that promote direct platform responsibility while maintaining democratic and sovereign oversight and accountability for action are most likely to meet the expectations of Canadians.

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content



# Global Regulatory Approaches to Online Harms

Designing regulatory interventions into the communication and information ecosystem of Canadians must be done with great care and in a manner that protects fundamental rights and freedoms. Learning the lessons from other jurisdictions around the world tackling these same issues should be top of mind.

In addition, an exclusive focus on content moderation can miss broader structural issues with modern online platforms, such as platform competition, personal data use by companies, and recommendation algorithms. However, it should also be acknowledged that some of these structural issues with the largest platforms are outside of meaningful influence from Canada alone. As such, Canada should try to align its regulatory efforts in the broader global context to the extent possible and support and coordinate efforts at international governance. A theme throughout our advice that follows is to align with other jurisdictions definitions or approaches to enable Canada to enhance, rather than detract from, a growing democratic force on these global platforms. To this end, we provide here a summary of the most relevant efforts by allied jurisdictions to govern online platforms and harms that we will reference in our advice.

n (de aux y 2004) (el matematica Notarional y contrata de la matematica Notarional y contrata de la matematica Inc. Accade de la matematica

# The United Kingdom

The governance model chosen by the UK and developed in a series of consultations with stakeholder groups is known as the 'duty of care'. Under this model, the UK's communications regulator Ofcom would oversee and enforce compliance with a standards framework designed by the government, in order to "ensure that companies continue to take consistent and transparent action to keep their users safe." Some commentators have argued that this duty of care required of tech platforms for online spaces is analogous to the duty of care required of property owners for their physical spaces.

The scope of the UK's duty of care framework is quite broad. The framework applies to all companies whose services host usergenerated content which can be accessed by users in the UK; and/or facilitate public or private online interaction between service. users, one or more of whom is in the UK, as well as search engines. However, this breadth is restrained by certain specific exceptions. For example, services that play a mostly 'functional' role in enabling online activity, such as ISPs, would not be subject to the framework. Perhaps most notably, journalistic content, as well as user comments on that content, would be specifically exempted in an effort to protect freedom of the press.

The harms proposed to be addressed by the duty of care framework are also quite broad. The framework targets criminal offences, harmful content affecting children, as well as content that can be harmful to adults even if legal. Disinformation and misinformation are also included in the framework, but only in situations in which that information could cause harm to individuals. Specifically out of scope are violations of intellectual property rights, data protection, fraud, consumer protection law, and cybersecurity breaches or hacking.

In terms of the specific actions that companies would need to take, any company that falls within the scope of the framework would be responsible for taking action to prevent usergenerated content on their platforms from causing physical or psychological harm to individuals. This would involve carrying out assessments of the risks associated with their services and taking action to reduce those risks.

If a user were to encounter harmful content on a platform which had an obligation under the framework to address that harm, then the user can report that harm and seek redress, such as content removal or sanctions against offending users, among other possibilities.

There would also be different obligations imposed on different 'classes' of companies. These classes would be determined by their degree of reach in the public media landscape, and therefore their potential to contribute to online harms. Such companies would have additional responsibilities under the framework, particularly with respect to the regulation of harmful content even when that content is not illegal. Among other differences, these companies would be required to regularly publish transparency reports in order to detail the approaches they had adopted to address online harms. The government explicitly stated that it would reserve the right to impose personal liability on the managers of tech companies in the event of failure to attain the standards of care specified by the regulator.

Rebailding Danada's Public Squarer Response to Government of Geneda's Proposed Approach to Actinese Normfol Contains

ne many series and an angle and many series of a more many Declaration of a series of the Mig. degree . As advantages

# The European Union

Like the UK, the EU has been moving toward a model of regulating online harms based largely on the idea that platforms should bear more responsibility when it comes to monitoring and addressing those harms. The EU's new approach to regulating online harms began with a 2018 recommendation document published by the European Commission. Building on the feedback from these recommendations, in December 2020 the European Parliament and European Council received a legislative proposal from the European Commission titled the Digital Services Act (DSA). It outlines a broad set of measures to regulate online platforms. What follows is a direct quotation of the stated intent of the legislation:

- measures to counter illegal goods, services or content online, such as a mechanism for users to flag such content and for platforms to cooperate with "trusted flaggers"
- new obligations on traceability of business users in online market places, to help identify sellers of illegal goods
- effective safeguards for users, including the possibility to challenge platforms' content moderation decisions
- transparency measures for online platforms on a variety of issues, including on the algorithms used for recommendations
- obligations for very large platforms to prevent the misuse of their systems by taking risk-based action and by independent audits of their risk management systems
- access for researchers to key data of the largest platforms, in order to understand how online risks evolve

 oversight structure to address the complexity of the online space: EU countries will have the primary role, supported by a new European Board for Digital Services; for very large platforms, enhanced supervision and enforcement by the Commission

While the new law upholds existing legal protections for platforms in terms of not being liable for the content they host in the EU, it also introduces a new responsibility to remove illegal content in a "timely, diligent and objective manner" once identified. As with the UK approach, the proposed EU model would operate using a tiered system, with larger platforms being subject to more stringent requirements. For example, platforms with over 45 million users would be required to abide by a range of new restrictions such as:

- Risk management obligations;
- External audits to assess the degree of risk for harm posed by the platform's activities;
- Transparency around recommendation systems related to user content;
- Obligations to share data with researchers to help understand online harms; and
- Cooperation with authorities in the event of crises.

For the first time in the EU, the law would specify that companies who fail to comply with these obligations would be subject to fines of up to 6% on their annual profits.

Rabailding Ganado's Public Squarer Response to Government of Ganada's Proposed Approach to Apdress Harmfol Content

ne an ann actain a' Mhainn Ioclamhal robaire Lann, a' G Ioclamhal robaire Lann, a' G

## Germany

In June 2017, the German Federal Parliament adopted the Network Enforcement Act or the NetzDG, which came into effect in October 2017. It should be noted that the law was adopted in a fast-tracked legislative process and was subject to significant criticism from civil society organizations. The law aimed to reduce hate speech, criminally punishable disinformation and other harmful content on social media. Under the Act, social networks with at least two million members in Germany are subject to multiple obligations. Most notably, the law requires social networks to remove or block access to content that is "manifestly unlawful" within 24 hours of receiving complaints unless provided otherwise by law enforcement. Social networks must also remove or block access to all other simply "unlawful" content generally within seven days of receiving a complaint, with certain exceptions involving whether the factual allegation is true or false or if the decision will be decided upon by an approved self-regulatory institution. The law also requires social networks to maintain effective and transparent organizational procedures for handling complaints about unlawful content available to users. Platforms designed to enable "individual communication or the dissemination of specific content" are specifically exempt from the law.

Rebuilding Ganada's Public Squaret Response to Government of Sanada's Proposed Approach to Address Harmful Contant

#### n (all arrysten) (andramatics) Coloring (1995) Coloring (1995) In Access for information

# Australla

Australia's eSafety Commissioner is dedicated exclusively to promoting online safety and enforcing compliance with online content moderation requirements under the *Enhancing Online Safety Act* (EOSA). The eSafety Commissioner was initially focused on promoting online safety for children, however in 2017, the Act was amended to expand the scope of its functions to include safeguarding against risks of online harm for all Australians.

Under the EOSA, the eSafety Commissioner is responsible for monitoring online platforms' compliance with safety requirements related to the cyber-bullying of children and nonconsensual sharing of intimate images. The EOSA requires social media service providers to include a provision that "prohibits endusers from posting cyber-bullying material" in its terms of use and a complaints framework under which users can report and request the removal of harmful material. Under the EOSA. if a material is considered a cyber-bullying act targeting an Australian child and the social media service does not remove the material within 48 hours of a complaint, the eSafety Commissioner has the power to request the removal of the material within 48 hours of a written notice. Moreover, the Commissioner has the power to issue an "end-user notice," under which the person posting the cyberbullying material is required to remove it and refrain from posting harmful content in the future. Civil penalties are enforced for failure to comply with the removal notice. The Commissioner can also invoke these regulatory powers to enforce the removal of intimate images shared without the subject's consent.

The eSafety Commissioner also has powers

under the Broadcasting Services Act (BSA) and the Criminal Code Act (CCA). Under the BSA, the Commissioner can investigate complaints and enforce the removal of "prohibited content" as defined by the Classification Board - the government body responsible for classifying films, publications, and online content, issuing age restrictions and implementing censorship auidelines. The Commissioner can issue a "removal notice" to a host of the illegal content in Australia, or a "blocking notice" to a local Internet Service Provider to prevent or restrict access to illegal content hosted outside of Australia. The Classification Board's definition of illegal content includes child abuse material, content promoting terrorism, and incitements of violence. Under the CCA, the Commissioner can request the removal of "abhorrent violent material," defined as content that records or streams terrorist acts, violence or kidnapping, and requires the internet, content, or hosting service provider to inform the Australian Federal Police "within a reasonable time after becoming aware of the existence of the material."

In June 2021, the Australian government enacted the Online Safety Act to once again expand the Commissioner's powers. The new legislation, which will come into effect in January 2022, expands the Commissioner's cyberbullying regulations to include adulttargeted cyber harms and requires the removal of cyberbullying material from a wide range of online services, not just social media sites. The new Act also grants the Commissioner enhanced powers to rapidly block websites that host abhorrent violent material in real time and reduces the timeframe required for service providers to comply with removal notices from 48 to 24 hours.

Rebailding Geneda's Public Squarer Response to Government of Geneda's Preprised Aparaboli to Aparese Harmfel Contain

# Our Advice on the Government's Current Proposal



We appreciate the opportunity to respond to the Government's proposed approach in detail. The following provides our recommendations to strengthen and clarify the proposal to ensure it best meets its objective of supporting a safe, inclusive and open online environment while protecting and advancing fundamental rights and freedoms.

Occument commonly in service In Consist Annaly & Uniformation Distancent released overward to the Access Reconstruction and

# Platforms in Scope

The Government's proposed definition of an "Online Communication Service" (OCS) to be in scope for this new law is "a service that is accessible to persons in Canada, the primary purpose of which is to enable users of the service to communicate with other users of the service, over the internet" and excludes "services that enable persons to engage only in private communications." The proposal provides regulatory power to the federal government to further specify the definition of an OCS, such as including or excluding a category of services and the meaning of the term private communications. The proposal's briefing material provides examples of platforms to be in scope, such as Facebook, YouTube, TikTok, Instagram and Twitter, while also providing examples of what it intends to exempt including telecommunications providers as well as private messaging, fitness, ridesharing and travel platforms.

# Platforms' Primary Purpose

The Government should consider clarifying its intentions by further defining what is meant by a service's "primary purpose" to ensure the very broad definition of user communication does not capture what it does not intend and that regulatory exemptions are not applied inconsistently. The Government may consider adopting language from the EU's proposed *Digital Services Act* (DSA) which clarifies platforms should not be in scope "where the dissemination to the public is merely a minor and purely ancillary feature of another service and that feature cannot, for objective technical reasons, be used without that other, principal service, and the integration of that feature is not a means to circumvent the applicability of the rules of this Regulation applicable to online platforms." Such language would clarify intentions with respect to services such as fitness, shopping or travel platforms.

Likewise, language from Germany's NetzDG and the UK's online harms bill aiming to protect freedom of the press and platforms exclusively dedicated to journalism could be adopted to specifically exclude "platforms offering journalistic or editorial content, the responsibility for which lies with the service provider itself." The EU's DSA preamble also specifies "the comments section of an online newspaper" as being exempt as an ancillary feature. The UK and Australia also both specifically exclude closed internal business platforms, which could be considered.

# Platform Size

As currently drafted, it appears that no size or user reach thresholds are proposed to exempt smaller platforms from the law. The Government should consider mirroring the platform size thresholds established in other jurisdictions that have been carefully crafted to prevent only entrenched incumbents with the resources to meet sophisticated regulatory requirements, as well as mitigate the risk of smaller platforms withdrawing their services, which could undermine freedom of expression and access to information.

The EU's DSA requires platforms of all sizes to have the basic ability for users to report illegal content, but exempts small platforms without significant reach from recourse and appeal mechanisms for such content, as well as transparency requirements.<sup>(5)</sup>

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content

Grassminnt commonique on viend ou la Lavisive Papage à Tarlannichan Dio commit enfectient d'arrayant to Die Viecess la internation deit

These are currently defined as enterprises employing fewer than 50 people with an annual balance sheet below EUR 10 million (\$15 million CAD) and fewer than 45 million average monthly active users in the EU (approx. 10% of population)." Germany's NetzDG has a threshold of two million registered users in Germany (approx. 2% of population) and also limits to platforms which have "profit-making purposes" to exempt non-profit and public enterprises." Australia's eSafety Commissioner can designate "large" platforms with legallybinding requirements while enabling others to participate on a cooperative basis; it has designated only three to date: Facebook, Instagram and YouTube."

Canada could potentially model this after similar size thresholds it established in the Canada Elections Act for online advertising transparency, which map closely to the EU's DSA thresholds and defines platforms in scope as those visited or used by Canadian users over the prior 12 months by an average of 3 million per month in English; 1 million per month in French; or 100,000 times per month in another language.

## Private Communication

The proposed exemption for "services that enable persons to engage only in private communications" captures an important and extremely complex element of this proposed law that potentially requires further clarification.

Many platforms offer both public and private communication functions, and clarification that blended platforms will have their different functions treated differently would help clarify scope. For example, Instagram is in scope but its direct message functions are not intended to be. Wording similar to the EU's *DSA* could be adopted: "Where some of the services provided by a provider are covered by this Regulation whilst others are not, or where the services provided by a provider are covered by different sections of this Regulation, the relevant provisions of this Regulation should apply only in respect of those services that fall within their scope."<sup>13</sup>

However, the distinction between public and private communications on many online platforms is not always clear. For example, is the proposal's intention to capture posts on social media that are private to only its followers (e.g., a private Facebook or Instagram profile or group)? If not, is it rational that regulatory action would be prioritized for content viewed by say a dozen people on a public profile over content viewed by thousands or millions on a private profile or group? To use another example, if a public Instagram profile posts a story to its close friends (a feature that limits access to a user-defined list of followers), is that post now private communication?

The EU's DSA attempts to make this public/ private distinction through its definition of "dissemination to the public" as "making information available, at the request of the recipient of the service who provided the information, to a potentially unlimited number of third parties" thereby exempting private profiles or groups." This has come under some scrutiny from experts; for example Caroline Cauffman and Catalina Goanta ask "should there not be a critical number of 'friends' or 'group members' that leads to the loss of confidentiality protection and to the same treatment as offers to or information shared with the public in general?" The EU's DSA is, however, not a consensus approach. Germany

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content exempts only "individual communication,"<sup>76</sup> the UK includes private profiles and messaging but excludes emails and SMS messages,<sup>77</sup> while Australia's approach includes all private communication.<sup>76</sup>

While thresholds at the individual level may be problematic, there may be no way to avoid establishing a threshold by what is considered private. For example, closed groups on Telegram can have up to 200,000 users, which surely stretches the meaning of "private" communication; however, one could envision all iMessage or Instagram message groups (each capped at 32 users) being considered private. However, we think it makes sense that this be left to regulations to evolve over time in consultation with experts and Canadians. One could also imagine the thresholds being different for different types of harms, for example a lower threshold for intimate images than other content.

Under the EU's DSA however, large private platforms that do not meet the "dissemination to the public" requirement are still required to have user-friendly mechanisms to electronically report content that users consider illegal, as well as provide notice to users if it removes or disables content, including the reasons for its decision and available redress possibilities. The law also still requires annual reports outlining their content moderation activities, including the number of user reports by type of alleged illegal content, action taken, and average time needed for taking action, as well as proactive measures taken as a result of the application and enforcement of their terms and conditions. Finally, when enabled by national laws, EU member states would also be able to order hosting services to remove illegal content.

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content



The Government should craft the legislation to enable a similar approach in which private platforms of a significant size are still subject to minimum requirements, such as user noticeand-action mechanisms and transparency requirements. This would better enable harm reduction, promote greater understanding of online harms, and would mitigate the risk of an incentive for companies to create more closed or private platforms as a means of sidestepping content moderation obligations. For a more detailed examination of potential regulatory mechanisms for online harms on private messaging apps, see *Private Messaging*. *Public Harms*.

### **Key Recommendations:**

- Clarify the online platforms in scope to exclude journalism platforms and platforms where user communication is a minor ancillary feature of a platform (e.g., fitness, shopping, travel)
- Establish platform size thresholds to place fewer obligations on smaller and non-profit platforms to avoid entrenching incumbents
- Require minimum standards of user reporting features and transparency for private platforms with very large user reach

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content

Dissument commonsplit on viewling In Levin Capage & Tellorminium Disconent intersect, overview to the Access formationistic with

# Harmful Content in Scope

The Government's proposal specifies five types of harmful platform content for which moderation will be regulated:

- 1. Terrorist content;
- 2. Content that incites violence;
- 3. Hate speech;
- 4. Non-consensual sharing of intimate images; and
- 5. Child sexual exploitation content,

These five categories are all worthy of regulatory action, though each is also very different, and the new regulator will need to develop expertise in each to meaningfully understand and implement the distinct categories of content.

The proposal refers to using Criminal Code definitions of this content "adapted to a regulatory context." The Government should engage experts and stakeholders further in these definitions given the very different contexts. For example, the proposed definition of content that incites violence is "actively encourages or threatens violence and which is likely to result in violence"; clarification may be needed as to whether coordination or recruitment to violence in absence of encouragement or threat is in scope, and whether this includes self harm. Darryl Carmichael and Emily Laidlaw also raise important questions about the definition of terrorist content in their submission."

We also think a sixth category of harmful content is worthy of consideration: identity fraud. Online impersonation is amongst the most common online harms, is often a poor fit

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content for the criminal justice system given the scale and speed of the platforms, and also has a clear Criminal Code definition ("fraudulently personates another person, living or dead, with intent to: gain advantage for themselves or another person; obtain any property or an interest in any property; or cause disadvantage to the person being personated or another person")." As an example, Facebook and Instagram reported in their most recent global transparency report that it actioned 1.7 billion fake accounts, compared to a combined total of 143 million accounts for hate speech, violent content, child endangerment and terrorism. YouTube also reports impersonation as a more frequent reason for channel removal than promotion of violence or terrorism. This could also enable the regulator to address an emerging threat to our democracy: synthetic media and deepfakes.

# **Key Recommendations:**

 Clarify the definitions of harmful content as it relates to online content moderation and consider adding identity fraud to list of harmful content in scope

Occument contribution on service le Lin six Pacade à Tatlornichen Do content referent ourcount to the Access to information an

## Content Moderation Requirements

The Government's proposal places obligations on platforms to "take all reasonable measures, which can include the use of automated systems, to identify harmful content that is communicated on its OCS and that is accessible to persons in Canada, and to make that harmful content inaccessible to persons in Canada." It also provides that platforms must take measures to ensure that the implementation and operation of the content moderation procedures, practices, rules, and systems put in place do not result in differential treatment of any group based on a prohibited ground of discrimination within the meaning of the Canadian Human Rights Act and in accordance with regulations. It also requires that content flagged by any person in Canada as harmful be addressed "expeditiously," which it indicates will be defined as 24 hours from the content being flagged or another period prescribed in regulations, including the ability to set different times for different types of harmful content. It requires a notice of decision to the user, the ability to compel a prompt review of the decision, and user notice of the reconsideration including the ability to appeal to the new Digital Recourse Council.

This proposed wording regarding "all reasonable measures" may be construed by platforms as a requirement to proactively monitor or filter all content accessible to persons in Canada, even from non-Canadians. This would have far-reaching implications. The UN's Special Rapporteur for Freedom of Opinion and Expression has criticized such general monitoring obligations as "inconsistent with the right to privacy and likely to amount to pre-publication censorship."" We believe

this provision needs to be reworked to be more narrow in scope, or at the very least, provisions in the EU's DSA should also be adapted, such as: "Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or active factfinding obligation, or as a general obligation for providers to take proactive measures to relation to illegal content" and "The removal or disabling of access should be undertaken in the observance of the principle of freedom of expression." Proposals have been advanced in the EU to clarify that monitoring obligations should only be enabled in specific cases such as blocking content which is identical to content which has previously been declared unlawful.<sup>36</sup> The UK's proposal also proposes to limit proactive monitoring only to child sexual abuse and terrorist content and requires all platforms to protect users' right to freedom of expression within the law when deciding on, and implementing, safety policies and procedures.

The proposed measures to ensure that monitoring obligations do not result in differential treatment or discrimination are positive features that somewhat mitigate risks. Consideration could be given to provide explicit authority to the new regulator to conduct independent audits of differential treatment. Cynthia Khoo's *Deplatforming Misogyny* provides excellent insights into ways to achieve substantive equality with respect to content moderation, or the notion that people in different positions may have to be treated differently to achieve true equality, that should also be considered.<sup>66</sup>

The current proposal is also asymmetrical with respect to user content wrongfully removed compared to harmful content that

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content

Ensetament commonlique no servir o la Las anchacada o Polifornal on Document integent portronal ro De secola ra micromistry ant

remains accessible; there is no regulated ability to appeal content removed or service suspended incorrectly under the platform's terms and conditions. The ability to appeal decisions to remove content through platform measures or automated systems is left at the discretion of the platforms, whereas illegal content that remains accessible is subject to a series of reporting and appeal mechanisms. This asymmetry is likely to incentivize more aggressive proactive filtering with implications for freedom of expression. To rebalance these incentives, the Government should also consider a complementary platform user notice and appeal mechanism for wrongful takedown or suspension of service and timely redress as is articulated in EU's DSA Article 17.3. It could also consider requiring users receive notices of when their content has been filtered or moderated through automated means, and the right to request that the platform's review of this decision be conducted through non-automated means.

Based on evidence to date, the 24 hour requirement for content decisions is likely to lead to over-censorship of non-harmful content." Even the Germany model only requires 24 hours for "manifestly unlawful" content and up to seven days to review other content." The EU's DSA also has a mechanism for "trusted flaggers" to have the content flagged prioritized for moderation, which Canada may wish to model.<sup>11</sup> We acknowledge the proposal already allows for regulatory flexibility in this regard, though we would advise explicit reference to 24 hours be removed. Instead, we would suggest the new regulator develop more precise requirements around the meaning of "expeditiously" in consultation with experts and stakeholders and reflecting the reality of how this new

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content law is implemented in Canada, including the effectiveness of the Recourse Council in providing guidance to platforms and improving democratic oversight of takedown decisions over time. The current proposal's structure may enable this, but the Government may also wish to consider focusing timely removal on content with more reach for certain types of harmful content or setting standards that aim to reduce the overall number of Canadians who see illegal content.

Finally, we would advise that a provision be explicitly added to ensure the user reporting and appeal mechanisms for illegal content are free of charge to the user throughout the process.

## **Key Recommendations:**

- 5. Narrow the requirement for platforms to take "all reasonable measures" to identify harmful content to avoid over-censorship and ensure wrongful takedown is appealable
- Ensure the length of time provided for content moderation decisions can evolve through regulatory changes

Occument communique en vernu de le Lui sur l'ennés è l'informetion Document milessett pursuant lo the Access in Minimation Acs

## Law Enforcement Reporting Requirements

The Government describes its proposal for mandatory law enforcement reporting as an 'interplay' between law enforcement and CSIS to identify public safety threats and prevent violence. The discussion guide acknowledges the limitations of content removal suggesting that it may be counterproductive by potentially pushing threat actors to encrypted platforms and away from the visibility and reach of law enforcement, thus producing more unmoderated harmful content. Although the potential of user migration to encrypted services is certainly a real phenomenon discussed further in our report Private Messaging, Public Harms, the Government's proposal does not give due credence to the challenges and potential harms of mandatory reporting to law enforcement operating in conjunction with automated content

The Government proposes two potential models for requiring platforms to report harmful content to law enforcement:

monitoring and removal.

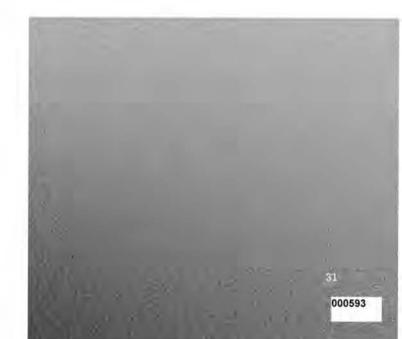
- a. when the platform has reasonable grounds to suspect the content reflects an imminent risk of serious harm to any person or to property; or
- b. when the platform believes content is illegal within the prescribed criminal offences of the five harmful content categories.

The first approach is consistent with the EU's DSA and many platforms' existing practices. The second approach intertwines content moderation with mandatory reporting, is too discretionary for platforms to meaningfully

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content

carry out without creating additional harm and should be abandoned. This approach risks disproportionately impacting racialized, religious minorities, LGBTQ+ people and other marginalized groups who, as Suzy Dunn has identified, are particularly at risk of having their content removed either deliberately through individuals who maliciously flag content or through content moderation systems that discriminate." Such groups could increasingly find themselves caught in a content removalpolicing nexus where their posts would be forwarded to law enforcement or CSIS for investigation, potentially unbeknownst even to the users themselves. The unintended consequences to free expression are not merely hypothetical. Google has challenged Germany's recent and similar proposal for violating fundamental human rights.<sup>31</sup> In addition, such an approach could undermine the equality-driven purpose of this legislation causing more harm to racialized and marginalized groups.

Even under the Government's first more limited proposal, regulatory clarity should be provided regarding the definitions of "reasonable grounds to suspect" and "serious harm" or else this proposal still risks undermining freedom of expression and the right to be secure against unreasonable search and seizure.



Grossminnt commonique on viend o la Lavisité canade à l'Information Do cument infeessett poissonnt to the Access la information 441

For example, the Electronic Frontier Foundation suggested in the EU context that user reports alone should not be sufficient to trigger obligations for reporting." Further, the subtext of this section seems focused on child sexual exploitation and terrorist content. We cannot foresee a scenario where automated filtering and reporting to law enforcement without victim consent of potential acts of hate speech or intimate images does not create more harm than good. We would urge considering limiting this section to be specific to the harmful content it intends to capture.

# **Key Recommendations:**

7. Limit any requirements for mandatory platform reporting to law enforcement to cases where imminent risk of serious harm is reasonably suspected and consider narrowing to only child sexual exploitation and terrorist content

## Platform Transparency Requirements

The Government's proposal requires platforms to produce reports on a scheduled basis to the new regulator providing Canada-specific data about several important elements, including:

- the volume and type of harmful content;
- · the volume and type of content moderated;
- the volume and type of content that was accessible to persons in Canada in violation of their community guidelines; and
- platforms' content moderation procedures, systems, resources, and activities.

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content These are important transparency provisions, and we would recommend that the legislation clarify these reports should be publicly accessible in a manner that respects individual privacy. The proposed provision regarding content "in violation of their community guidelines" is well-intentioned, though we think it would be clearer to replace 'community guidelines' with 'terms and conditions' as community guidelines is a term only used by some platforms. It would also be strengthened if "the volume and type of content moderated" was ideally split between automated and human moderation.

Mandated and audited transparency is among the most powerful platform governance tools that governments have. It would also be beneficial for these requirements to be built in cooperation with international allies to ensure data can be compared to other countries to the extent possible, as well as leave regulatory flexibility for the new regulator to add additional transparency requirements that advance their overall mandate in consultation with experts, allies, and stakeholders.

## **Key Recommendations:**

8. Ensure platform transparency requirements are publicly accessible in a manner that respects individual privacy and work with international allies to ensure data comparability

Disetament connectionague no senare la Leo escritación e Polarmation Disturment referente overvient ro Une secono la contempilar, sec

# **New Regulators**

The Government proposes to create a new regulatory body in the Digital Safety Commission to administer and enforce these requirements, as well as engage in partnerships, education outreach activities and research. It also proposes the establishment of the Digital Recourse Council to review and issue content moderation decisions, as well as an Advisory Board to support and advise the Commission and the Recourse Council. The Commissioner will have broad inspection and enforcement powers, including the ability to recommend fines of up to the higher of 3% of global revenue or \$10 million to the body responsible for administering privacy violations, or to refer fines to prosecutors of up to 5% of global revenue or \$25 million.

The design of the regulatory and oversight bodies seems fit for purpose, though of course the devil will be in the details of how these new bodies are implemented, adequately resourced, and use their authorities. For example, there may be considerable complaint volume at the Recourse Council, so we wonder if it would be best to leave the maximum number of members (currently prescribed as five) as flexible in the regulations.

It is worth noting that the functions of the Digital Safety Commission seem deliberately broader than just the five prescribed types of harmful content, which is positive and will hopefully allow the Commission to engage in partnerships and research on broader issues of digital safety not yet in scope for regulatory action (e.g., disinformation harmful to public safety, synthetic media or automated/bot content labelling, ad transparency, doxing, algorithmic transparency, etc.). It would also seem to enable the Digital Safety Commissioner to engage in partnerships with civil society and international allies; one could envision investigations or partnerships with European and Australian digital commissioners on matters of joint interest.

The broad inspection powers proposed for the Commission may satisfy this, but the Government may consider adopting the more specific provisions in the EU's *DSA* Article 31 to compel very large platforms (defined as more than 10% of the population or 450 million monthly active users) to cooperate with independent research, including providing data to vetted academic researchers and specific data security and confidentiality requirements, including provisions relating to trade secrets. These EU provisions are world-leading and the Government should ensure Canadian researchers can similarly engage in better understanding online platforms.

The Government should also consider mirroring the EU's DSA Articles 26 and 27 that requires very large platforms to annually review and put in place mitigation measures for their systemic risks in: the dissemination of illegal content; any negative effects for the exercise of the fundamental rights and freedoms; and intentional manipulation of their service with effects on the protection of public health, minors, civic discourse, electoral processes and public security.<sup>77</sup> These provisions enable their Commission to produce an annual report with the most prominent and recurrent systemic risks and best practices for mitigation. Like in the financial services industry, compelling companies to review their potential risks to society can be a powerful tool for mitigation.

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content

### **Key Recommendations:**

 Require larger platforms to cooperate with independent researchers and annually review and mitigate their systemic risks

# Website Blocking

The Government's proposal also enables the Commissioner to apply to the Federal Court for an order to block access to a platform, in whole or in part, that demonstrates persistent noncompliance with orders regarding child sexual exploitation or terrorist content. Site-blocking powers have understandably been met with significant criticism by internet service providers and civil society organizations for censorship, impairing individual liberty, and potentially exacerbating harm against the marginalized populations that the law in part seeks to protect." This proposed power requiring judicial authorization is guite prescribed, though it is worth noting that Germany and the EU's approach do not contain this power relying on monetary penalties,<sup>201</sup> and Australia only has site-blocking powers for time-limited viral distribution of terrorist content in response to the Christchurch Call. The Government may also wish to review the UK's proposed approach that enables blocking of 'ancillary' services such as payment processing, advertising services and search results for a site, as a means to pressure compliance before outright blocking.<sup>100</sup>

It is not clear that this measure is necessary, effective and proportionate, given that major platforms increasingly appear to be

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content in compliance with removal requirements for unlawful content. For example, in an evaluation of the European Commission's Code of Conduct on countering illegal hate speech online, companies removed on average 70% of illegal hate speech notified to them, with companies meeting the target set of reviewing the majority of notifications within 24 hours, reaching an average of more than 81% (and figures for both have steadily increased with each evaluation)." Recognizing that the existing provision allows for site blocking to be "in part", many of the platforms proposed to be in scope host far more legal expression than illegal, so enabling site-blocking only of platforms where the majority or significant proportion of content is non-compliant could also be a way to narrow scope and mitigate Charter scrutiny.

## **Key Recommendations:**

10. Remove or significantly narrow the ability to block access to platforms for non-compliance

# About the Authors

Sam Andrey is the Director of Policy & Research at the Ryerson Leadership Lab. Sam has led applied research and public policy development for the past decade, including the design, execution and knowledge mobilization of surveys, focus groups, interviews, randomized controlled trials and crosssectional observational studies. He also teaches about public leadership and advocacy at Ryerson University and George Brown College. He previously served as Chief of Staff and Director of Policy to Ontario's Minister of Education, in the Ontario Public Service and in not-for-profit organizations advancing equity in education and student financial assistance reform. Sam has an Executive Certificate in Public Leadership from Harvard's John F. Kennedy School of Government and a BSc from the University of Waterloo.

Alexander Rand is interested in disinformation and the ways in which new technologies influence online political discourse. He has worked as a Public Policy Researcher at the Centre for the Future of Democracy, and at the London-based AI think tank Future Advocacy. He holds a Master of Public Policy from Cambridge University, where he conducted statistical analyses of online partisanship and disinformation in the Canadian context, as well as a BA from McGill University in Economics and Music Technology.

Mohammed (Joe) Masoodi is a Senior Policy Analyst in the Ryerson Leadership and Cybersecure Policy Exchange. Joe has been conducting research and policy analysis on the intersections of surveillance, digital technologies, security and human rights for over six years. He has conducted research at the Surveillance Studies Centre at Queen's University and the Canadian Forces College. He holds an MA in war studies from the Royal Military College of Canada, an MA in sociology from Queen's University, and has studied sociology as a PhD candidate from Queen's University, specializing in digital media, information and surveillance.

Karim Bardeesy is the Co-Founder and Executive Director of the Ryerson Leadership Lab. Karim is a public service leader who has worked in progressively senior roles in public policy, politics, journalism and academia in Toronto and the United States since 2001. He is also a board member of The Atmospheric Fund and Corporate Knights, Inc., a member of the Banff Forum, and a founding faculty member of Maytree Policy School. Karim was previously Deputy Principal Secretary for the Premier of Ontario, the Honourable Kathleen Wynne, and served as Executive Director of Policy for Premiers Wynne and Dalton McGuinty. He has worked as a journalist, an editorial writer at The Globe and Mail, and as an editorial assistant at Slate magazine. Karim holds a Master in Public Policy from Harvard's John F. Kennedy School of Government.

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content

# Methodology

Three anonymous online surveys were conducted with random samples of research study panelists in Canada to better understand Canadians' views on online harms and regulation:

> 2019: 3,000 Canadian residents aged 18 and over from August 1-7, 2019 conducted by Abacus Data from a set of panels based on the Lucid exchange platform and Leger panel

2020: 2,000 Canadian residents aged 18 and over from May 14-22, 2020 conducted by Pollara Strategic Insights using the AskingCanadians panel

2021: 2,500 Canadian residents aged 16 and over from March 17-22, 2021 conducted by Abacus Data from a set of panels based on the Lucid exchange platform Response quotas were set and the data were weighted according to the latest Canadian census data to ensure that the sample matched Canada's population according to age, gender, educational attainment and region. Totals may not add up to 100 due to rounding. As a guideline, a probability sample of this size would yield results accurate to  $\pm$ 2 percentage points, 19 times out of 20.

The 2019 survey was supported by the Governments of Canada and Ontario. The 2020 survey was supported by RBC. The 2021 survey was supported by RBC and the Government of Canada.

paganeers communique en servir à la pro-auty autor : Follomict an De conserve case d'autorité de De sector la communité de la

# **Survey Questions**

#### Figure 1: Which best describes how often do you do the following?

- About once an hour
- A few times a day
- Daily
- A couple times a week
- Once a week
- Once every few weeks
- A few times a year
- I don't do this/use this service
- Unsure/don't know
- a. Watch news on TV
- b. Listen to the news on the radio
- c. Listen to a podcast
- d. Visit a news website
- e. Open a news app on your mobile device
- f. Read something on Wikipedia
- g. Read a print newspaper
- h. Read a print magazine
- i. Use Google Search
- j. Use Google News
- k. Use Facebook Newsfeed
- I. Use Facebook Messenger
- m. Use LinkedIn
- n. Use Instagram
- o. Use Pinterest
- p. Use Reddit
- q. Use Snapchat
- r. Use Tumblr
- s. Use Twitter
- t. Use WeChat
- u. Use WhotsApp
- v. Watch something on YouTube

Figure 2: Have you used any of the following messaging apps in the last year?

1

m.

'n.

0.

٠

.

٠

.

b.

C.

Instagram

Reddit

Twitter

p. YouTube

LinkedIn

Figure 5: Thinking of any online

information (websites, Facebook,

etc.), how often do you think you

Twitter, Instagram, news apps,

encounter the following?

A few times a week

A few times a month

Unsure/don't know

biased information

biased information

divisive content

Less than once a month

a. Deliberately false information

Deliberately misleading or

d. Accidentally misleading or

e. Deliberately inflammatory or

Accidentally false information

Every day

Once a week

Once a month

Never

sources for news or political

- Yes
- No
- Don't know or prefer not to say
- a. WhatsApp
- b. Facebook Messenger
- c. WeChat/Weixin
- d. Telegram
- e. Signal
- f. Snapchat
- g. Direct messages on Instagram
- [Viber/imo/Weibo]\*
- [LINE/Discord/Clubhouse]\*
- [QQ/Direct messages on Twitter/
- Direct messages on TikTok]\*
- \* Survey respondents split into
- three and each asked one of each
- Figures 3 and 4: Which of the following do you use to stay up to date with the news or current events? (select all that apply)
- a. An email newsletter
- Messages from friends, family or colleagues (e.g., text, WhatsApp, Facebook Messenger)
- c. TV
- d. Radio
- e. Podcasts
- f. Print newspapers
- g. Print magazines
- h. News websites
- i. News alerts on my mobile device
- Search engine (e.g., Google, Bing, etc.)
- k. Facebook

divisive content a. Something you

f.

g. Something you would consider hate speech

Accidentally inflammatory or

- h. Something you would consider racist content
- i. Something you would consider sexist content
- Something you would consider violent content

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content

Figure 6: Proportion of respondents to question in Figure 5 who chose Facebook/YouTube/Twitter in question to Figures 3 and 4

Figure 7: [only asked to those who indicated using at least one private messaging app] Thinking about all the messaging apps you use, how often do you think you receive messages, including links, images or videos, that contain what you would consider:

- Every day
- A few times a week
- A few times a month
- A few times a year
- Never
- Don't know or prefer not to say
- a. Information about the news or current events that you immediately suspect to be false
- Information about the news or current events that you believe to be true and later find out is at least partly false
- c. Hate speech that wilfully promotes hatred against an identifiable group
- d. Harassment or bullying
- e. A scam (e.g., phishing to provide personal information or to download malware)
- f. Promoting or encouraging violence

Figure 8: Question from Figure 5, in addition to: Which of the following actions have you done?

- Yes
- No
- I think so
- Unsure

- a. Fact checked a post about the news on a different site
- b. Blocked or muted an account or phrase
- Reported or flagged an account or post for hateful content
- d. Reported or flagged an account for being fake/ automated
- e. Reported or flagged a post for being false
- f. Downloaded an ad-blocker or privacy app to track data being shared with third parties
- g. Change the settings on each app/platform so that your profile is less public

Do you consider yourself a member of a visible minority / racialized community?

Figure 9: Below we have a list of specific companies or services. We want you to think about whether each of these make decisions that you consider to be in the best interest of the public, and others that you consider to care less about what is in the best interest of the public.

On a scale of 1-9, where 1 means you have no trust at all and 9 means you have a high degree of trust, how do you feel about each of the following when it comes to trusting them to act in the best interest of the public:

- a. Amazon
- b. Apple
- c. Bell Canada
- CBC / Radio-Canada [split outside/inside of Quebec; n=1,854/597]

- e. National Post / La Presse [split outside/inside of Quebec]
- f. CTV/TVA [split outside/inside of Quebec]
- g. Toronto Star / Le Journal de Montreal [split outside/inside of Quebec]
- h. Facebook
- i. Globe and Mail
- j. Global News
- k. Google (Alphabet Inc.)
- I. Imperial Oil / Shell Canada [split sample; n=1,168/1,283]
- m. Instagram
- n. Microsoft
- o. Tim Hortons
- p. TikTok
- q. Twitter
- r. Wikipedia
- s. WhatsApp
- t. YouTube

Figure 10: Below is a list of organizations that often handle data about Canadians. How much do you trust these organizations to keep your personal data secure? Rate on a scale of 0 to 10, with 0 being "Do not trust at all" and 10 being "Completely trust".

- a. The federal government
- b. Your provincial government
- c. Your municipal government
- d. Health care providers (e.g., hospitals, doctors)
- e. The police
- f. Banks
- g. Telecommunication providers (e.g., Bell, Rogers, Telus)
- h. Apple
- i. Facebook
- j. Google
- k. Microsoft

# Figure 11: Please indicate which of the following best describes your perspective:

- Protecting freedom of expression is more important than regulating speech online.
- Reducing the amount of hate speech, harassment and false information online is more important than free expression.
- Social media platforms should be held responsible when they allow posting of inaccurate or illegal content in the same way that news media are held responsible.
- People who post inaccurate or illegal content on social media platforms should be held responsible, not the platforms.
- Government should intervene in social media companies to require the companies to fix the problems they have created in our political system.
- Government should have no role in intervening in social media companies.

#### Figure 12: There have been a number of actions proposed to address some of the challenges with social media today. For each of the following, would you say you strongly support, somewhat support, are neutral, somewhat don't support or strongly don't support:

 Requiring platforms to delete accounts that intentionally spread disinformation

- Requiring platforms to delete accounts that impersonate others
- Requiring platforms to delete illegal content in a timely manner, like hate speech, harassment and incitement of violence
- Requiring platforms to develop third-party fact-checking verification of news and warning users when something is not true
- e. Requiring that users be able to control how their social media feeds are presented to them, such as chronologically
- f. Increasing digital and media literacy education for Canadians
- Increasing public subsidies
   for journalism and public
   broadcasting
- Requiring that automated content or bot accounts be banned
- Requiring platforms identify paid promoted content and its source
- Requiring a public database of social media content by political parties or registered third parties
- Banning targeted online advertisements during an election period
- Requiring that links be clicked on before they can be shared
- Breaking up big social media companies like Facebook into smaller entities

If the Canadian government were to introduce some of these actions and they had the following impacts on Facebook's operations (which includes Facebook, Messenger, Instagram and WhatsApp), would this make you much more, somewhat more, somewhat less, or much less supportive of the government getting involved? If it would have no impact, please say so.

- Much more supportive
- Somewhat more supportive
- No impact
- Somewhat less supportive
- Much less supportive
- Don't know or prefer not to say
- a. Facebook shutting down operations in Canada
- b. Facebook charging a monthly
   \$5 fee in order to operate in
   Canada
- Facebook delaying your posts
   by a few minutes to review the content

# References

1 Canadian Race Relations Foundation. (2021, January 25). Poll demonstrates support for strong social media regulations to prevent online hate and racism. https://www.orrf-forr.ca/en/ news-a-events/media-releases/item/27349-poll-demonstratessupport-for-strong-social-media-regulations-to-prevent-onlinehate-and-racism

2 Garneau, K. & Zossou, C. (2021, February 2). Misinformation during the COVID-19 pandemic. *Statistics Canada*. https:// www150.statcan.gc.ca/n1/pub/45-28-0001/2021001/ article/00003-eng.htm

3 Owen, T. et al. (2021, January 5). Understanding Vaccine Hesitancy in Canada: attitudes, beliefs, and the information ecosystem. *Media Ecosystem Observatory*, https://files. cargocollective.com/c745315/meo\_vaccine\_hesistancy.pdf

4 Humphreys, A. (2020, July 3). Man who allegedly crashed truck through Rideau Hall's gate with four guns is soldier troubled by COVID conspiracies. *National Post*. https://nationalpost.com/ news/man-who-allegedly-crashed-truck-through-rideau-hallsgate-with-four-guns-is-soldier-troubled-by-covid-conspiracies

5 Canadian Commission on Democratic Expression. Harms Reduction: A Six-Step Program to Protect Democratic Expression Online. (2021, January). *Public Policy Forum*. https://ppforum.ca/ wp-content/uploads/2021/01/CanadianCommissionOnDemocra ticExpression-PPF-JAN2021-EN.pdf

6 It's time to block hate online. (n.d.). *Blockhate*. https://blockhate. co

7 Canadian Coalition to End Online Hate. (n.d.). Centre for Israel and Jewish Affairs. https://www.cija.ca

8 Housefather, A. (2019, June), Taking action to end online hate. Report of the Standing Committee on Justice and Human Rights. 42nd Parliament, 1st Session. House of Commons. https:// www.ourcommons.ca/Content/Committee/421/JUST/Reports/ RP10581008/justrp29/justrp29-e.pdf

9 Laidlaw, E. (2015, August), Regulating Speech in Cyberspace: Gatekeepers, Human Rights, and Corporate Responsibility. *Cambridge University Press*, https://www.cambridge.org/core/ books/regulating-speech-in-cyberspace/7A1E83C71D0D67D13 756594BE3726687

10 Examining the impact of digital technologies on Canadian society. (n.d.). *Democratic Expression*. https://www. commissioncanada.ca

11 Carmichael, D. & Laidlaw, E. (2021, September 13). The Federal Government's Proposal to Address Online Harms: Explanation and Critique. *University of Calgary Faculty of Law*, https://ablawg. ca/2021/09/13/the-federal-governments-proposal-to-addressonline-harms-explanation-and-critique/

12 Stecula, D., Pickup, M., & van der Linden, C. (2020, July 6). Who believes in COVID-19 conspiracies and why it matters. *Policy Options*. https://policyoptions.irpp.org/magazines/july-2020/whobelieves-in-covid-19-%20conspiracies-and-why-it-matters/

13 Suárez, E (2020, March 31). How fact-checkers are fighting coronavirus misinformation worldwide. *Reuters Institute*, https:// reutersinstitute.politics.ox.ac.uk/risj-review/how-fact-checkersare-fighting-coronavirus-misinformation-worldwide

14 Edelman, G. (2020, December 27). Better Than Nothing: A Look at Content Moderation in 2020. *Wired*. https://www.wired.com/

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content story/content-moderation-2020-better-than-nothing/

15 Draft Online Harms Bill 2021, pt. 2. https://assets.publishing. service.gov.uk/government/uploads/system/uploads/ attachment\_data/file/985033/Draft\_Online\_Safety\_Bill\_ Bookmarked.pdf

16 Department for Digital, Culture, Media & Sport. (2020, December 15). Online Harms White Paper. Full government response to the consultation. *Government of the United Kingdom.* https://www.gov.uk/government/consultations/onlineharms-white-paper/outcome/online-harms-white-paper-fullgovernment-response

17 Woods, L., & Perrin, W. (2019, April). Online harm reduction – a statutory duty of care and regulator. *Carnegie UK Trust.* https://d1ssu070pg2v9i.cloudfront.net/pex/pex\_ carnegie2021/2019/04/06084627/Online-harm-reduction-astatutory-duty-of-care-and-regulator.pdf

18 Online Harms White Paper, 2020

19 Ibid.

20 Ibid.

21 Draft Online Harms Bill 2021, pt. 2 c. 6.

22 Online Harms White Paper, 2020

23 Ibid

24 Ibid

25 Draft Online Harms Bill 2021, pt. 2 c. 2

26 Ibid

27 Online Harms White Paper, 2020

28 Ibid

29 Draft Online Harms Bill 2021, pt. 3 c. 1.

30 Online Harms White Paper, 2020

31 Europe fit for the Digital Age: Commission proposes new rules for digital platforms. (2020, December 15). Press Release. *European Commission*. https://ec.europa.eu/commission/presscorner/detail/en/ip\_20\_2347

32 Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. COM/2020/825 final. https://eur-lex.europa.eu/legal-content/en/ TXT/?gid=1608117147218&uri=COM%3A2020%3A825%3AFIN

33 Digital Services Act 2020, c. III s. 1 a. 11. https://eur-lex.europa.eu/legal-content/en/ TXT/?gid=1608117147218&uri=COM%3A2020%3A825%3AFIN

34 Digital Services Act 2020, c. III s. 4 a. 25.

35 Digital Services Act 2020, c. III s. 4 a. 26-33

36 Digital Services Act 2020, c. IV s. 3 a. 59

37 Germany: Flawed Social Media Law. (2018, February 14). Human Rights Watch. https://www.hrw.org/news/2018/02/14/ germany-flawed-social-media-law 38 Kettemann, M. (2019, May). Follow-up to the comparative study on "blocking, filtering and take-down of illegal internet content". Leibniz-Institute for *Media Research & Hans-Bredow-Institut*. https://rm.coe.int/dgi-2019-update-chapter-germany-study-onblocking-ond-filtering/168097ac51

39 Network Enforcement Act 2017, a. 1 s. 1. https://www.bmjv.de/ SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG\_ engl.pdf;isessionid=BBE250F3A09040DF3193FEC171E78E06.2\_ cid297?\_\_blob=publicationFile&v=2

40 Network Enforcement Act 2017, s. 3.

41 Network Enforcement Act 2017, s. 3.

42 Kettemann, M. (2019, May). Follow-up to the comparative study on "blocking, filtering and take-down of illegal internet content". Leibniz-Institute for *Media Research & Hans-Bredow-Institute*, 4. https://rm.coe.int/dgi-2019-update-chapter-germany-study-onblocking-and-filtering/168097ac51

43 Network Enforcement Act 2017, a. 1 s. 3

44 Network Enforcement Act 2017, a. 1 s. 1

45 eSafety Commissioner. (n.d.) Government of Australia. Our Legislative Functions. https://www.esafety.gov.au/about-us/whowe-are/our-legislative-functions

46 Ibid.

47 Enhancing Online Safety Act 2015 (Cth) pt 3. https:// www.legislation.gov.au/Details/C2018C00356/Html/Text#\_ Toc524097331

48 Enhancing Online Safety Act 2015 (Cth) pt 5A. https:// www.legislation.gov.au/Details/C2018C00356/Html/Text#\_ Toc524097331

49 Enhancing Online Safety Act 2015 (Cth) pt 4. https:// www.legislation.gov.au/Details/C2018C00356/Html/Text#\_ Toc524097331

50 Enhancing Online Safety Act 2015 (Cth) pt 4 div 2. https:// www.legislation.gov.au/Details/C2018C00356/Html/Text#\_ Toc524097331

51 Enhancing Online Safety Act 2015 (Cth) pt 5. https:// www.legislation.gov.au/Details/C2018C00356/Html/Text#\_ Toc524097331

52 Enhancing Online Safety Act 2015 (Cth) pt 4 div 2-3. https:// www.legislation.gov.au/Details/C2018C00356/Html/Text#\_ Toc524097331

53 Enhancing Online Safety Act 2015 (Cth) pt 5A – Non-Consensual Sharing of Intimate Images. https://www.legislation. gov.au/Details/C2018C00356/Html/Text#\_Toc524097331

54 Broadcasting Services Act 1992 (Cth) pt 4 div 1-2. https:// www.legislation.gov.au/Details/C2021C00042/Html/Volume\_2#\_ Toc62734656

55 Department of Infrastructure, Transport, Regional Development, and Communications. Government of Australia. *Classification Ratings*. https://www.classification.gov.au/ classification-ratings/what-do-ratings-mean

56 Online Safety Act 2021 (Cth) pt 9. https://parlinfo.aph.gov. au/parlInfo/download/legislation/bills/r6680\_first-reps/toc\_ pdf/21022b01.pdf;fileType=application%2Fpdf

57 Online Safety Act 2021 (Cth) pt 8 div 3. https://parlinfo.aph.

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content gov.au/parlInfo/download/legislation/bills/r6680\_first-reps/toc\_ pdf/21022b01.pdf;fileType=application%2Fpdf

58 eSafety Commissioner. (n.d.) Government of Australia: Illegal Harmful Content. https://www.esafety.gov.au/key-issues/Illegalharmful-content

59 Criminal Code Act 1995 (Cth) pt 10.6 div 474.32 https://www. legislation.gov.au/Details/C2021C00066/Html/Volume\_2#\_ Toc63237533

60 Criminal Code Act 1995 (Cth) pt 10.6 div 474.33 https://www. legislation.gov.au/Details/C2021C00066/Html/Volume\_2#\_ Toc63237533

61 eSafety Commissioner. (n.d.) Government of Australia. Our Legislative Functions. https://www.esafety.gov.au/about-us/whawe-are/our-legislative-functions

62 Online Safety Act 2021 (Cth) pt 3 div. 4. https://parlinfo.aph. gov.au/parlInfo/download/legislation/bills/r6680\_first-reps/toc\_ pdf/21022b01.pdf;fileType=application%2Fpdf

63 eSafety Commissioner. (n.d.) Government of Australia. *Our Legislative Functions*, https://www.esafety.gov.au/about-us/who-we-are/our-legislative-functions

64 Online Safety Act 2021 (Cth) pt 8 div 3. https://parlinfo.aph. gov.au/parlInfo/download/legislation/bills/r6680\_first-reps/toc\_ pdf/21022b01.pdf;fileType=application%2Fpdf

65 Online Safety Act 2021 (Cth) pt 9. https://parlinfo.aph.gov. au/parlInfo/download/legislation/bills/r6680\_first-reps/toc\_ pdf/21022b01.pdf;fileType=application%2Fpdf

66 Digital Services Act 2020, s.13

67 Network Enforcement Act 2017, a. 1 s. 1.

68 Digital Services Act 2020, s.13

69 Digital Services Act 2020, Explanatory Memorandum, s.2

70 Ibid

71 Network Enforcement Act 2017, a. 1 s. 1 -2.

72 eSafety Commissioner. (n.d.). Government of Australia. Working with social media: https://www.esafety.gov.au/about-us/ consultation-cooperation/working-with-social-media

73 Digital Services Act 2020, s.15

74 Digital Services Act 2020, c.1 a.2 s.(i)

75 Cauffman, C. & Giants, C. (2021, April 15). A New Order: The Digital Services Act and Consumer Protection. *Cambridge University Press.* https://www.cambridge.org/core/journals/ european-journal-of-risk-regulation/article/new-order-the-digitalservices-act-and-consumer-protection/8E34BA8A209C61C42A1 E7ADB6BB904B1

76 Network Enforcement Act 2017, a. 1 s. 1.

77 Draft Online Harms Bill 2021, p. 2 c. 6

78 Online Safety Act 2021 (Cth) pt 1 s.13A

79 Carmichael, D. & Laidlaw, E. (2021, September 13). The Federal Government's Proposal to Address Online Harms: Explanation and Critique. *University of Calgary Faculty of Law*. http://ablawg. ca/wp-content/uploads/2021/09/Blog\_DC\_EL\_Federal\_Online\_ Harms\_Proposal.pdf 80 Criminal Code, RSC 1985, c C-46, s. 403(1)

81 Community Standards Enforcement Report. (n.d.). Transparency Center (Q2 2021). *Facebook* https://transparency. fb.com/data/community-standards-enforcement/

82 YouTube Community Guidelines Enforcement. (n.d.) Transparency Report. Goog/e. https://transparencyreport.google. com/youtube-policy/removals?hl=en

83 Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. (2018, April 6). Presented to HRC, 38th session. *United Nations Human Rights Office of the High Commissioner*. https://www.ohchr.org/EN/ Issues/FreedomOpinion/Pages/ContentRegulation.aspx

84 Digital Services Act 2020, s. 28

85 Digital Services Act 2020, s. 22

86 European Parliament. (2021, June 21). Committee on Culture and Education. https://www.europarl.europa.eu/doceo/ document/CULT-PA-693943\_EN.pdf

87 Draft Online Safety Bill 2021, p.4 c.4

88 Khoo, C. (2021). Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence. *Women's Legal Education and Action Fund*. https://www.leaf.ca/ publication/deplatforming-misogyny/

89 Keller, D. (2021, February 8). Empirical evidence of overremoval by internet companies under intermediary liability laws: an updated list. *The Centre for Internet and Society*. http:// cyberlaw.stanford.edu/blog/2021/02/empirical-evidence-overremoval-internet-companies-under-intermediary-liability-laws

90 Network Enforcement Act 2017, a.1 s.3

91 Digital Services Act 2020, s.3 a.19

92 Geist, M. (Host). (2021, August 23). "They Just Seemed Not to Listen to Any of Us" – Cynthia Khoo on the Canadian Government's Online Harms Consultation (No. 99). [Audio podcast episode]. *In Law Bytes*. https://www.michaelgeist. ca/2021/08/law-bytes-podcast-episode-99/

93 Google takes legal action over Germany's expanded hate-speech law. (2021, July 27). *Reuters*. https://www.reuters. com/technology/google-takes-legal-action-over-germanysexpanded-hate-speech-law-2021-07-27/

94 Digital Services Act Proposal: Recommendations for the EU Parliament and Council. (2021). *Electronic Frontier Foundation*. https://www.eff.org/files/2021/05/07/dsa\_recommendations\_ parliament\_council.pdf

95 Digital Services Act 2020, s.4 a.31

96 Digital Services Act 2020, s.4 o.26-27

97 "Specific groups or persons may be vulnerable or disadvantaged in their use of online services because of their gender, race or ethnic origin, religion or belief, disability, age or sexual orientation. They can be disproportionately affected by restrictions and removal measures following from (unconscious or conscious) biases potentially embedded in the notification systems by users and third parties, as well as replicated in automated content moderation tools used by platforms." *Digital Services Act 2020*, s. 3. https://eur-lex.europa.eu/legal-content/en/ TXT/?uri=COM:2020:825:FIN

Rebuilding Canada's Public Square: Response to Government of Canada's Proposed Approach to Address Harmful Content 98 Network Enforcement Act 2017, a. 1 s. 4.

99 Enhancing Online Safety Act 2015 (Cth) pt 4 div 2-3.

100 Barbaschow, A. (2020, March 24). ISPs to continue blocking graphic violent content in Australia. *ZDNet*, https://www.zdnet. com/article/isps-to-continue-blocking-graphic-violent-contentin-australia/

101 Online Safety Bill 2021 (Cth). https://assets.publishing.service. gov.uk/government/uploads/system/uploads/attachment\_data/ file/985033/Draft\_Online\_Safety\_Bill\_Bookmarked.pdf

102 Countering illegal hate speech online - Commision initiative shows continued improvement, further platforms join. (2018, January 19). Press Release. *European Commission*, https://ec.europa.eu/commission/presscorner/detail/en/IP\_18\_261

Document communiqué en vertu de la Loi sur l'accès à l'information Document released pursuant lo the Access to Information Act.

# DELETING DIGITAL HARM:

# A REVIEW OF NOVA SCOTIA'S CYBERSCAN UNIT

# ALEXA DODGE, PHD

AUGUST 2021



**About the Author:** Alexa Dodge is a Hill Postdoctoral Fellow in Law, Justice, & Society at Dalhousie University. She researches legal, restorative, and educational responses to digital forms of sexual violence, harassment, and bullying. This report shares the findings of her current research exploring informal responses to cyberbullying and nonconsensual intimate image distribution through an analysis of Nova Scotia's CyberScan unit.

For questions or media inquiries regarding this report please contact: alexa.dodge@dal.co



#### This research was approved by the Dalhousie University Research Ethics Board REB # 2020-5209

Cite as: Dodge, Alexa (2021). Deleting Digital Harm: A Review of Nova Scotia's CyberScan Unit. Holifax: Dalhausie University.

## TABLE OF CONTENTS

DEFINITIONS
EXECUTIVE SUMMARY & INTRODUCTION
METHODS
HISTORY OF CYBERSCAN
TAKING A RESTORATIVE APPROACH?
COMMUNICATING CYBERSCAN'S ROLE
TYPES OF CASES RESPONDED TO
COMPLAINANT & RESPONDENT DEMOGRAPHICS
NUMBER OF CASES RESPONDED TO
CYBERSCAN'S RELATIONSHIP TO CIVIL & CRIMINAL JUSTICE PROCESSES
Use of civil court orders
RELATIONSHIP TO CRIMINAL RESPONSES
MOST COMMON RESPONSES
IMAGE/CONTENT TAKEDOWN AND TECHNOLOGICAL KNOW-HOW
EMOTIONAL SUPPORT & INFORMATION
RESPONSES TO YOUTH CASES
SCHOOL-BASED RESPONSES TO YOUTH COMPLAINANTS & RESPONDENTS
EDUCATIONAL PRESENTATIONS
EDUCATION REGARDING NONCONSENSUAL INTIMATE IMAGE DISTRIBUTION
LABELLING YOUTH INTIMATE IMAGES AS "CHILD PORNOGRAPHY"
INFORMING NATIONAL RESPONSES TO DIGITAL HARM
REFERENCES

#### DEFINITIONS

*Cyberbullying:* "An electronic communication, direct or indirect, that causes or is likely to cause harm to another individual's health or well-being where the person responsible for the communication maliciously intended to cause harm to another individual's health or well-being or was reckless with regard to the risk of harm to another individual's health or well-being"<sup>1</sup>.

*Nonconsensual Intimate Image Distribution:* "To publish, transmit, sell, advertise or otherwise distribute" a private nude, semi-nude or sexually explicit image "(i) knowing that the person in the image did not consent to the distribution, or (ii) being reckless as to whether that person consented to the distribution"<sup>2</sup>.

*CyberScan Unit:* The CyberScan unit is a government enforcement unit within the Province of Nova Scotia's Department of Justice. CyberScan agents provide "informal" supports to complainants who are experiencing cyberbullying and nonconsensual intimate image distribution, help complainants navigate civil or criminal law options when applicable, and provide educational presentations on cyberbullying and nonconsensual intimate image distribution to Nova Scotians.<sup>3</sup>

#### EXECUTIVE SUMMARY & INTRODUCTION

There is growing recognition internationally of the harms associated with cyberbullying and nonconsensual intimate image distribution. In Canada, much of the government response to these issues has focused on legal responses as a core solution (e.g. the federal *Protecting Canadians from Online Crime Act* (2014) and various civil law remedies at the provincial level). Although new criminal and civil law options may lead some to believe that these issues are now adequately addressed, this report finds that legal remedies are often unappealing to many complainants and are unable to address the core issues that underly acts of cyberbullying and nonconsensual distribution. Legal responses do not provide the expedient technological and emotional supports that many victims most desire and they can be counterproductive by bringing additional and extended attention to harmful content. As legal remedies are less widely used and desired than is often assumed, it is necessary to consider what alternatives to traditional legal responses may be available. Therefore, this report analyzes Nova Scotia's CyberScan unit to explore the efficacy of their primarily informal responses to cyberbullying and nonconsensual intimate image distribution.

The CyberScan unit, a government enforcement unit that primarily provides "informal" responses to cyberbullying and nonconsensual intimate image distribution, represents a rare example of a government response to harm that does not require engagement with the legal system. This report provides a detailed description and analysis of the successes and shortcomings of the CyberScan unit as it currently operates. This report will be useful not only for Nova Scotian's seeking to reflect on the accomplishments and room for improvement in responding to cyberbullying and

<sup>&</sup>lt;sup>1</sup> Intimate Images and Cyber-protection Act, SNS 2017, c 7, para 3(c).

<sup>&</sup>lt;sup>2</sup> Intimate Images and Cyber-protection Act, SNS 2017, c 7, para 3(d).

<sup>3</sup> https://novascotia.ca/cyberscan/

nonconsensual intimate image distribution in the province, but also for national and international audiences considering implementing alternative responses to these digital harms.

This report details the history of the CyberScan unit (See: <u>History of CyberScan</u>), the types of cases the unit responds to (See: <u>Types of cases responded to</u>), and the various responses the unit offers. As detailed below, the unit was originally created in 2013 as part of the enactment of Nova Scotia's *Cyber-safety Act*. Following the striking down of this act as unconstitutional in 2015, the role of the unit changed to some extent and now operates under the *Intimate Images & Cyber Protection Act* (2017). Under CyberScan's current mandate, CyberScan agents are primarily tasked with providing "informal" supports to complainants who are experiencing cyberbullying and nonconsensual intimate image distribution (See: <u>Most common responses</u>), helping complainants navigate their civil or criminal law options when applicable (See: <u>CyberScan's relationship to civil & criminal justice processes</u>), and providing education and information about cyberbullying and nonconsensual intimate image distribution to Nova Scotians (See: <u>Educational presentations and Communicating CyberScan's role</u>).

While part of CyberScan's mandate is to help victims of cyberbullying or nonconsensual distribution navigate the civil or criminal law responses available to them, this report finds that the vast majority of complainants who contact CyberScan are not interested in engaging in legal processes. Rather, the most common response complainants request is help to remove/report nonconsensually posted intimate images or cyberbullying content from websites or social media platforms. CyberScan agents explain that the expedient removal of harmful content is top of mind for most complainants and, often, no additional action is requested. The second most common resource complainants are looking for is emotional and informational support. CyberScan agents report that it can be a comforting and validating experience for complainants to simply speak with someone who has knowledge of these digital harms and can assure complainants that they are not at fault for having been victimized, that many others have experienced these harms and have found support, and that they do not have to deal with this alone. Much more rarely, complainants are interested in having CyberScan contact the respondent to attempt to stop acts of cyberbullying or nonconsensual distribution by informing respondents of the harm they are causing and/or describing the potential legal consequences of their actions. CyberScan agents report that in almost all cases these informal supports are able to resolve the issue to the complainant's satisfaction and legal processes are not required or desired. The fact that most cases are resolved without recourse to legal remedies (and that most complainants do not desire legal remedies) demonstrates the need for alternatives to legal responses.

While CyberScan is clearly providing vital and in-demand informal responses and support options, this report details several recommendations for improving the unit's responses. Some of the recommendations given in this regard include:

- Provide CyberScan agents with training on best practices for supporting complainants or respondents who are in distress/crisis.
- Provide CyberScan agents with training on best practices for supporting victims in those cases that include acts of sexual violence (e.g. sexualized cyberbullying, nonconsensual intimate image distribution).

- Expand the unit's hours of operation to ensure expedient responses to complainants seeking help to report/remove harmful content, and link to alterative content takedown resources that complainants can access outside of CyberScan's hours of operation.
- Consider hiring additional CyberScan agents to allow for the provision of expedient and holistic responses.
- Re-establish connections with restorative approaches initiatives in the province to provide responses to digital harm that are holistic, forward-focused, inclusive/participatory, and relationship-focused (See: <u>Taking a restorative approach?</u>).
- Ensure CyberScan's website and resource materials accurately explain the range of supports they provide and avoid overemphasizing the legal options that complainants rarely utilize (i.e. better highlight the technological and emotional supports offered).
- Provide resources to help parents/guardians, teachers, and other potential supporters learn best practices for non-judgementally supporting a victim of cyberbullying or nonconsensual intimate image distribution.
- Make the unit more accessible to youth complainants by removing the requirement for youth under the age of 18 to have parental permission to speak with CyberScan.
- Make the unit more accessible to youth complainants by offering options for contacting the unit without having to make a phone call (i.e. offer options to contact the unit through text, live online chat, email, and/or messaging apps).
- Use individual cases of digital harm as a catalyst to consider what systems-level changes are needed to address the broader issues revealed by an individual case (e.g. sexist cyberbullying among a group of teenagers could be used as a catalyst to address sexist beliefs throughout their school's student body and in their school's policies and practices).
- Use CyberScan's experience attempting to report/remove harmful content from various websites and social media platforms to help inform federal initiatives on platform and website responsiveness to takedown requests.

In addition to CyberScan's responses to individual cases of digital harm, the unit is also tasked with providing educational presentations on cyberbullying and nonconsensual intimate image distribution. CyberScan's educational presentations are mainly delivered to youth and take the form of "cyber safety" presentations (See: Educational presentations). The "cyber safety model" of education primarily responsibilizes potential victims to protect their online privacy and to avoid online interactions with strangers, making it largely ineffective at addressing the kind of peer-to-peer cyberbullying and nonconsensual intimate image distribution that is most common among youth. The cyber safety model of education does not address the discriminatory beliefs and relational conflict that often underly acts of cyberbullying and nonconsensual intimate image distribution. Additionally, cyber safety education that focuses primarily on discussions of the victims' role in avoiding harm can be counterproductive by invisibilizing the actions of perpetrators and implying that the culture that supports bullying is natural and unchangeable (Fairbairn et al., 2013; Mishna et al., 2020). Best practices in addressing cyberbullying and nonconsensual intimate image distribution assert that education should be focused on teaching the importance of healthy/ethical relationships, equality/inclusion, consent, and empathy (Fairbairn et

# al., 2013; Choo, 2015; Johnson, 2016). Therefore, this report provides several recommendations for a major reworking of CyberScan's approach to education, such as:

- Move away from the "cyber safety" model of education and instead seek to address the core discriminatory and relational issues that underly cyberbullying and nonconsensual distribution.
- In collaboration with schools and community organizations, provide ongoing and interactive education on healthy/ethical relationships, equality/inclusion, consent, and empathy.
- Avoid using scare tactic approaches and, instead, help youth feel empowered to make change, seek support, and support others.
- When educating on the topic of nonconsensual intimate image distribution, avoid victimresponsibilizing / anti-sexting approaches that can increase the shaming and blaming of victims. Instead, focus on the importance of consent and respecting the privacy and bodily autonomy of others (See: Education regarding nonconsensual intimate image distribution).
  - When educating on the topic of nonconsensual intimate image distribution among youth, avoid framing this act as "child pornography" (See: <u>Labelling youth intimate images as</u> "child pornography").

As detailed in this report, there are several ways in which the CyberScan unit could improve its responses to cyberbullying and nonconsensual intimate image distribution. However, the core supports provided through CyberScan's support line role (i.e. technological and emotional supports for complainants) seem to be a successful and in-demand resource. CyberScan's work in this regard could be used as a model to provide all Canadians with this kind of support line (See: Informing national responses to digital harm). Somewhat comparable services are available in the UK through the Revenge Porn Helpline and in Australia through the national eSafety Commissioner, but Canada does not currently have a national program that provides supports and resource hub, the recommendations in this report could also be useful for exploring the kinds of preventative education and restorative responses that a federal program might help nurture at the local level. Both CyberScan's successes and shortfalls offer a useful guide for considering best practices in responding to and preventing the harms of cyberbullying and nonconsensual intimate image distribution.

#### METHODS

The methodology for this report includes interviews and document analysis. Semi-structured interviews were completed with four CyberScan staff in 2016<sup>4</sup> (one complaints coordinator and three government enforcement agents) and three CyberScan staff in 2020 (one complaints coordinator and two government enforcement agents)<sup>5</sup>. To ensure interviewees could speak openly

<sup>&</sup>lt;sup>4</sup> One agent was interviewed in 2021 regarding their work with the unit up to and including 2016.

<sup>&</sup>lt;sup>5</sup> In 2016 the CyberScan unit had 6 staff, but not all staff were available for interviews due to frequent travel for work. In 2020 the CyberScan unit had only 3 staff and all staff members were available for interviews.

about both the successes and challenges that they perceived in the CyberScan approach, interviewees were anonymized and are all referred to as "agents". Agents are cited using the following anonymous codes:

- CyberScan interviewees from 2016: CS1; CS2; CS3; CS4
- CyberScan interviewees from 2020: CS5; CS6; CS7

Interviews were also conducted in 2021 with two restorative approaches experts that have provided guidance to the CyberScan unit. These restorative approaches experts are referred to using the following anonymous codes:

Restorative approaches interviewees from 2021: RA1; RA2

The CyberScan website and CyberScan resources were also analyzed. This includes:

- CyberScan's website at: https://novascotia.ca/cyberscan/
- What you need to know about the Infimate Images and Cyber-Protection Act (PDF)
- Here to help: CyberScan unit (PDF)
- CyberScan's infographic on Public Outreach Results
- CyberScan's PowerPoint slides used in educational presentations for youth

#### HISTORY OF CYBERSCAN

The CyberScan unit was created in 2013 as part of the enactment of Nova Scotia's Cyber-safety Act<sup>6</sup>. The Cyber-safety Act was created in response to the tragic death of Rehtaeh Parsons<sup>7</sup> and other high-profile cases<sup>8</sup> in which young people died by suicide in the aftermath of cyberbullying and/or nonconsensual intimate image distribution. The Cyber-safety Act created both civil law and informal remedies for cases of cyberbullying and nonconsensual intimate image distribution. It established a tort for cyberbullying, set out the procedure for complainants to apply for a Cyberbullying Protection Order, amended the Education Act to ensure that schools address cyberbullying behaviour occurring on or off school property that is disruptive to the school environment, and amended the Safer Communities and Neighbourhoods Act to create the CyberScan unit. The CyberScan unit was authorized to investigate complaints of cyberbullying, send warning letters to respondents, apply for Cyberbullying Prevention Orders, provide advice and support to complainants (e.g. through helping to remove cyberbullying content posted online), and attempt to resolve complaints through negotiation or informal agreement. In addition to the responsibilities described in the Cyber-safety Act, the CyberScan unit was also tasked with providing educational presentations about cyberbullying to Nova Scotians and acting as a resource for schools responding to incidents of cyberbullying.

<sup>&</sup>lt;sup>6</sup>Cyber-safety Act, S.N.S. 2013, c. 2.

<sup>&</sup>lt;sup>7</sup>The death of Nova Scotian teenager Rehtaeh Parsons was the main catalyst for creating the legislation that resulted in the CyberScan Unit (Taylor, 2016). Parsons died by suicide in the aftermath of having an intimate image of her (captured during an alleged sexual assault) nonconsensually distributed and used as fodder for sexist and victim blaming/shaming bullying and harassment by her peers.

<sup>&</sup>lt;sup>8</sup> Nova Scotia was also at the forefront of discussing issues of digital harm prior to the Rehtaeh Parsons case. As Choo (2015) explains, "after the deaths of teenagers, Jenna Bowers-Bryanton, Courtney Brown and Emily McNamara in 2011, the provincial government created a task force to look into the prevalence of cyberbullying" (p. 68).

In 2015 the *Cyber-safety Act* was struck down by the Supreme Court of Nova Scotia. In *Crouch v Snell* (2015), the *Cyber-safety Act* was found unconstitutional based on sections 2(b) (Freedom of expression) and 7 (Life, liberty, and security of the person) of the *Charter*. In his decision, Justice McDougall referred to the *Act* as "a colossal failure"<sup>9</sup>. A core issue was the overly broad definition of cyberbullying provided in the *Cyber-safety Act*, though other important issues were also detailed by the court (See: Taylor, 2016). David Fraser, the privacy lawyer who challenged the *Act*, was happy to see this particular legislation struck down as he asserts: "I consistently heard from and about people whose political or legitimate *Charter*-protected speech was removed from the internet because members of CyberScan bullied the people into removing it under threat of unspecified 'legal action' that could include removing their internet access" (Fraser, 2017). While the civil law and investigative powers of CyberScan were immediately removed by the striking down of this legislation, the CyberScan unit remained partially active during this time as they were able to continue providing educational presentations and could provide complainants with information (e.g. instructions on how to report a nonconsensually distributed intimate image to a social media company, contact information for counselling in their community).

In 2018 a redrafted version of the Act, with a narrower definition of cyberbullying and explicit reference to nonconsensual intimate image distribution, came into force as the Intimate Images & Cyber Protection Act (2017)<sup>10</sup>. While this current legislation still allows complainants to apply for civil law remedies through a Cyber-Protection Order<sup>11</sup>. CyberScan staff can no longer apply for orders on behalf of complainants and the CyberScan unit is no longer tasked with investigative powers or the authority to send formal warning letters. Rather, the new CyberScan mandate focuses even more explicitly than the original mandate on providing informal resolutions and victim supports. The new mandate under the Intimate Images & Cyber Protection Act describes the following role for CyberScan: "(a) provide public information and education regarding harmful on-line conduct; (b) advise public bodies on policies for online safety and conduct; (c) provide support and assistance to victims of intimate image distribution without consent and cyberbullying: (d) provide information to victims of intimate image distribution without consent and cyber-bullying respecting the criminal justice system and proceedings under this Act; (e) provide information to victims of intimate image distribution without consent and cyber-bullying respecting contacting police; (f) provide voluntary dispute-resolution services, including advice, negotiation, mediation and restorative justice approaches in respect of harmful on-line conduct: and (g) provide such other services, exercise such other powers and authorities and perform such other duties as may be prescribed by the regulations"12.

Although CyberScan's powers are much more limited under the current *Intimate Images & Cyber Protection Act* than under their original mandate, the unit's work in practice has not changed as drastically as might be assumed. From its inception to the present day the CyberScan unit has primarily provided informal responses/supports and educational presentations. Despite this, most scholarly and media attention has focused on CyberScan's (no longer active) powers regarding

8

<sup>9</sup> Crouch v. Snell, 2015 NSSC 340, para 165.

<sup>&</sup>lt;sup>10</sup> Intimate Images and Cyber-protection Act, SNS 2017, c 7.

<sup>&</sup>lt;sup>11</sup> Complainants can apply for a Cyber-protection Order to, for instance, order a respondent to remove cyberbullying posts and forbid the respondent from contacting the complainant.

<sup>&</sup>lt;sup>12</sup> Intimate Images and Cyber-protection Act, SNS 2017, c 7, para 12.

civil orders and formal warning letters and little attention has been paid to their informal and educational responses. This report provides a more fulsome understanding of CyberScan's approach by detailing the unit's relationship to civil and criminal law processes as well as the unit's primarily informal and educational responses.

# TAKING A RESTORATIVE APPROACH?

Provincial Minister of Justice Mark Furey has stated that CyberScan uses a "restorative approach" in its responses to cyberbullying and nonconsensual intimate image distribution. In 2017 he stated that the province will "continue to help victims with restorative approaches through the CyberScan Unit<sup>13</sup> and in 2020 he stated that CyberScan applies a "restorative justice methodology"<sup>14</sup>. As the Intimate Images & Cyber Protection Act (2017) came into force, provincial politicians<sup>15</sup> and the director of CyberScan also highlighted the use of restorative approaches (Tutton, 2018). Despite these expressions that CyberScan takes a restorative approach, members of the CyberScan unit themselves do not recall having received directives or resources to work restoratively and suid they would not refer to their current response as taking a restorative approach (CS5, CS6). There seems to be a disconnect between the government's stated intention in this regard and the response provided in practice. One of the restorative approaches experts interviewed for this report suggested that this disconnect could be due to a misunderstanding of what it means to take a restorative approach: "There seems to be an understanding expressed by the government that because CyberScan isn't criminal or punitive focused that they must be restorative, rather than robustly thinking of a restorative approach as a relational approach that looks at the contexts, causes, and circumstances [surrounding a harmful act]" (RA2). Based on the robust restorative approaches that have been championed in the province of Nova Scotia, responses that are called restorative might be expected to be grounded in the following guiding principles: relationship focused; inclusive and participatory; comprehensive/holistic; and forward-focused (RA1).

Although CyberScan does not seem to offer a robust restorative approach in practice, attempts were made in the early stages of envisioning the CyberScan unit to meaningfully connect CyberScan into ongoing restorative initiatives in the province. Most notably, several experts in restorative approaches pushed for CyberScan's work to align with the restorative response to bullying that was already implemented in many Nova Scotian schools (RA2). These experts argued that responses to "cyberbullying" should align with existing restorative responses to "offline" bullying because "cyberbullying is not something completely different from [offline bullying]" (RA2). Both bullying and cyberbullying, they asserted, generally have relational issues at their core and any strict distinction between the two creates a "false divide" that does not reflect the lived reality for "kids [who] carry their devises all the time" (RA2). This assertion is supported by research that has found that young people, like many adults, now understand their "online" and "offline" lives as seamlessly integrated (Boyd, 2014) and that "cyber" and "offline" forms of bullying are significantly interrelated (Mishna & Van Wert, 2015). This early push for CyberScan to take a restorative approach resulted in a professional development day for school principals aimed at bringing CyberScan's response to cyberbullying into harmony with the significant

9

<sup>&</sup>lt;sup>13</sup>Nova Scotia, Legislative Assembly, Hansard, 63rd Leg, 1st Sess, No 27 (26 October 2017) at 1828-9.

<sup>14</sup> Nova Scotia, Subcommittee of the Whole on Supply, Hansard (9 March 2020).

<sup>&</sup>lt;sup>15</sup> Nova Scotia, Legislative Assembly, Hansard, 63<sup>rd</sup> Leg, 1<sup>st</sup> Sess, No 27 (12 October 2017).

existing work on bullying in schools. The following is an excerpt from a handout used in the resulting "CyberScan and Schools" professional development day that was held shortly before CyberScan became fully active in September of 2013:

Schools, government, community agencies, students and families need to build the collaborative relationships essential to addressing and responding to cyberbullying in order to ensure safety and security. The appropriate processes and responses required in the event of cyberbullying may differ on a case-by-case basis depending upon the needs of the students, families, school communities and the range of circumstances and factors involved. The following guiding principles allow the collaboration necessary to craft an appropriate response:

#### **Relationship Focused:**

- CyberSCAN and schools should understand cyberbullying relationally and respond by examining the relationships involved in and affected by the situation.
- A response cannot focus on individual students without considering the others involved and affected by the situation including those within the school community, families and wider community.
- The response will focus on the harm caused to students and others and harmful patterns or structures
  of relationship; not simply on the breech of rules or laws.

#### **Inclusive and Participatory:**

- A focus on the relationships between and among those involved requires processes that are inclusive and participatory and culturally proficient.
- Responses will not only identify who was hurt and who was directly responsible but will inquire who
  else was impacted or involved and who is essential to responding to the situation and assuring a safe
  and successful outcome. This can include families, school and community supports and other resources.

#### Comprehensive/Holistic:

 A comprehensive and holistic approach to understanding a cyberbullying incident means considering the context and causes along with the broad ranging effects related to an incident.

#### Forward-focused:

Responses will approach cyberbullying in a problem-solving and solution focused way. They will
focus on understanding what happened including the context, causes and contributing factors of
cyberbullying and on determining the appropriate response to ensure that it does not continue.

The focus will be on facilitating and supporting parties to understand and take appropriate responsibility for their actions, address the harmful effects of their actions and commit to a plan to ensure safe and respectful relationships in future.

The above document demonstrates that, when the unit was first being envisioned, there were initial attempts to connect CyberScan into the network of people taking a restorative approach in Nova Scotia. Despite this early work, CyberScan agents interviewed in both 2016 and 2020 did not describe receiving directives, training/professional development, or resources related to providing a robust restorative approach and did not describe their approach as restorative. Those working under the original CyberScan legislation did describe working closely with school principals to respond to cases among youth which, considering the work on restorative approaches being taken in many schools at that time, may have resulted in agents working restoratively in some ways. However, as described in more detail below (See: <u>School-based responses to youth complainants & respondents</u>), CyberScan agents' responses to cases in schools do not seem to follow restorative

principles and, rather, seem to often rely on legal warnings and "cyber safety" presentations<sup>16</sup> that do not address the relational conflict or discriminatory beliefs that are at the core of many acts of cyberbullying and nonconsensual distribution.

Agents in 2020 said that, although CyberScan itself does not necessarily take a restorative approach, the Community Justice Society has recently invited CyberScan agents to participate in a few restorative justice responses to cases involving aspects of cyberbullying. Their role in these processes has involved "trying to get [the perpetrator] to think about how their online behaviour can really impact people" and, at times, providing a "one-on-one educational session with the youth to talk about online behaviour" (CS5). This is one way that CyberScan has recently made some connection with the restorative justice processes occurring in Nova Scotia; However, there are much broader ways that CyberScan could link into restorative approaches in the province. As one of the restorative approaches experts explained in terms of restorative responses in schools:

"Some people think that unless you bring [the victim and perpetrator] together in a circle, you didn't take a restorative approach. But you can take a restorative approach [while having] very few circles. It's not one particular process that makes an approach restorative, but rather it is about taking that lens that asks 'What is going on in the background here? Stop that behaviour please because it's harmful, but tell us what is actually going on.' [...] We have to debunk the myth that taking a restorative approach to cyberbullying would mean 'Oh we will just bring in the victim and the perpetrator and we're going to put them in a circle', but rather it looks like asking 'What is going on here? How do we invite participants into this process in a safe way? [...] How do you bring in the caregivers of the alleged perpetrator [...] in a way that they understand that we are not just looking for a punitive response here, but we are looking to have your child come in and participate in a process to respond to something that is having very serious impacts on somebody else?" (RA1)

Although CyberScan does not currently work in a particularly restorative manner, there are several reasons to believe that this would be a useful direction to move toward. CyberScan agents described that the vast majority of cases they respond to involve complainants and respondents who are known to each other, primarily as schoolmates, (ex)friends, (ex)partners, work colleagues, or neighbours (CS4, CS5); Therefore, the relationship focused responses offered by restorative approaches could provide appropriate tools for addressing the impacts on relationships that result from digital harms. In addition to the relevance of relationship focused responses, restorative approaches are also useful because they seek to address the systems-level issues that influence acts of cyberbullying and nonconsensual distribution. For instance, if an act of cyberbullying involved sexist comments, a restorative approach would seek to address not just the ways sexist beliefs negatively impacted the relationships between the particular youths involved, but would also look at how the school as an institution is normalizing gender inequality. One of the restorative approaches experts explained how a school culture might send the message that gender inequality is acceptable by, for instance, emphasizing male sports over female sports: "If we are structuring [our sports funding] around gender than we are clearly signaling that girls and boys are unequal.

<sup>&</sup>lt;sup>16</sup> As discussed further in the section on <u>Educational presentations</u>, these presentations do not seem to engage youth in discussion about the rights of others, diversity, consent, or healthy relationships. Rather, these presentations focus primarily on teaching potential victims how to secure their online privacy.

So with this approach [...] you need to be thinking about all of what is happening in your building" (RA1). This interviewee explained that it is often necessary to respond expediently to cases to immediately stop the initial harm (e.g. immediately stopping the spread of nonconsensually distributed intimate images), but those responding must then be "willing to sit down and say 'What the heck is going on here relationally? How are things structured here so that that person thought that was a tool that they ought to be able to use without consequences?" (RA1). In this way, individual moments of harm become catalysts for asking broader questions, such as: "What needs to change in this building? What do we learn from this situation? [Do we need to change] a policy or practice in the building? What different conversations do we need to be having with our students?" (RA1). This approach holds individuals "to account in a meaningful way" while also seeking to "look at the collective responsibility for an incident" (RA1).

Restorative responses are necessary to account for and address the relational issues. discriminatory beliefs, policies, and practices that fuel and aggravate the harms associated with cyberbullying and nonconsensual intimate image distribution. Evidencing this, restorative responses were a core recommendation of the Standing Senate Committee on Human Rights' report Cyberbullying Hurts: Respect for Rights in the Digital Age (2012). Recognizing the importance of restorative approaches, this report will consistently reflect on how CyberScan's responses might better connect with the robust restorative principles and resources developed in Nova Scotia. There are certainly ample opportunities for CyberScan to "consider [a restorative] approach to their work and to be a catalyst to building those kinds of responses" (RA2). Through building relationships with and working alongside those in Nova Scotia who are part of an "ecosystem of restorative supports", CyberScan could access "supports to work in more holistic, integrated ways with a really robust set of resources and experiences" (RA2). The new Restorative Research, Innovation and Education Lab could provide a first contact to help CyberScan reconnect with those working restoratively in the province. Engagement with restorative approaches will not involve finding some new "perfect solution" for CyberScan to utilize, rather it will help CyberScan to continuously consider opportunities to improve their responses (RA2).

> Recommendation #1: Re-establish CyberScan's connection to Nava Scotia's network of restorative approaches initiatives in schools and communities.

## COMMUNICATING CYBERSCAN'S ROLE

All CyberScan agents reported that CyberScan responds to the vast majority of cases through "informal responses" (i.e. responses that do not involve any use of laws or interaction with the justice system). In rare cases that are not resolved informally, agents working under the Cyber-safety Act (2013) had the power to send formal warning letters to respondents and to apply for civil court orders on behalf of complainants, while agents working under the Intimate Images and Cyber-protection Act (2017) no longer have these powers (See: Use of Civil Court Orders). While these changes in terms of formal responses are important in some cases, they are not as impactful to CyberScan's work as might be assumed because the unit has always provided informal responses to the vast majority of their cases. By far the most common responses that CyberScan agents provide, and that complainants are looking for, are technological and emotional support (See: Most common responses). Much more rarely, agents attempt to resolve issues by contacting

respondents to attempt to stop cyberbullying or nonconsensual distribution by explaining the harm the respondent is causing and/or the potential legal consequences of their actions. Even more rarely, CyberScan helps complainants navigate their civil or criminal law options. CyberScan agents consistently explained that most complainants do not want the respondent contacted and even fewer want to initiate a legal response. Although CyberScan's most in-demand responses are technological and emotional support for complainants, these supports are often not mentioned when communicating CyberScan's role to the public. For instance, the CyberScan website currently describes CyberScan's resources in the following way: "CyberScan staff can help victims find a solution to a dispute involving cyber-bullying or the sharing of intimate images. They can contact the person who shared the images or cyberbullied the victim to try to resolve the matter informally using dispute resolution, including advice, negotiation, mediation and restorative practices. [...] CyberScan can also help victims navigate the justice system and understand their options".<sup>17</sup> This explanation does not mention emotional support and help with content takedown. and rather focuses on the much more rarely desired options of contacting respondents and engaging the justice system. While information on rarely used options should certainly be included as they will be useful to a small number of complainants, the current framing of the unit's role could discourage those who are not looking to engage the respondent or begin a legal process from contacting CyberScan. The above quote also mentions that respondents can be engaged through "mediation and restorative practices", vet CyberScan agents in 2020 report that they have never convened a victim-offender mediation session and that they would not describe the unit as engaging in restorative practices.

When explaining how CyberScan can help in the document What you Need to Know about the Intimate Images and Cyber-protection Act, there is some mention of providing general "support" to complainants; However, help with content takedown is still not mentioned and the emphasis continues to be on responses that engage respondents or utilize civil law. This is demonstrated in the following section from this document: "CyberScan staff can contact the person who distributed the intimate images without consent or who engaged in cyberbullying to explain the process and try to solve the matter informally using restorative practices or other approaches. They can also help you to navigate the justice system, help you understand your options, offer you support, and try to solve the matter informally using restorative practices or other approaches"18. The second document linked to on CyberScan's website, titled Here to Help: CyberScan Unit also places a great deal of emphasis on civil law options. For instance, rather than describing some of the ways that CyberScan can provide immediate emotional and technological supports, this document says to call CyberScan to "learn how to apply for a court order or for more information on additional supports"<sup>19</sup>. This document describes the informal options available saying "CyberScan will seek to resolve the matter informally using restorative practices or other approaches"<sup>20</sup>. CyberScan's website and documents should be updated to speak more fully and accurately to the reality of what CyberScan offers in terms of responses (e.g. clarify what kinds of "mediation and restorative practices", if any, they offer) and to highlight their most in-demand supports (e.g. support in reporting/removing harmful content and emotional support).

<sup>17</sup> novascotia.ca/cyberscan

<sup>&</sup>lt;sup>18</sup> What you need to know about the Intimate Images and Cyber-Protection Act (PDF), p.3.

<sup>&</sup>lt;sup>19</sup> Here to help: CyberScan unit (PDF), p.4.

<sup>&</sup>lt;sup>20</sup> Here to help: CyberScan unit (PDF), p.2.

Considering CyberScan's mandate to provide education on cyberbullying and nonconsensual intimate image distribution, their website should also be updated to provide links to useful educational resources on these issues. CyberScan agents expressed that they would like to have additional resources to make their website more of an educational and informational hub, however they do not feel that they currently have the capacity to do such work (the unit currently operates with half the staff of the original CyberScan unit). One agent suggested that, with more capacity, they would like to provide comprehensive and regularly updated resources akin to those provided on the website for Australia's eSafety Commissioner (CS5). Although this kind of robust educational hub would require more resources. CyberScan's site could easily be updated to link to existing Canadian organizations that provide comprehensive and evidence-informed educational and support resources. For instance, the MediaSmarts<sup>21</sup> website provides extensive information for youth, parents, and teachers on best practices for education about and support in response to eyberbullying and nonconsensual intimate image distribution. If CyberScan were to develop a more robust educational approach as discussed further below (See: Educational presentations) their website could also communicate the ways that agents could help interested parties to craft educational workshops or resources specific to their school or community's needs.

> Recommendation #2: CyberScan's website and materials should be updated to accurately reflect the responses they offer and to highlight the options that complainants are most often seeking.

> Recommendation #3: The CyberScan website should link to comprehensive and evidence-informed educational and support resources on the issues of cyberbullying and nonconsensual intimate image distribution.

## TYPES OF CASES RESPONDED TO

This section provides an overview of the kinds of cases CyberScan responds to. The first subsection describes the demographics of complainants and respondents and the relationship between complainants and respondents in CyberScan cases. The second subsection describes the number of cases CyberScan responds to. And the third subsection describes the types of digital harm CyberScan responds to.

### COMPLAINANT & RESPONDENT DEMOGRAPHICS

Because the CyberScan unit emerged in response to high-profile cases of cyberbullying and/or nonconsensual intimate image distribution among young people, it is often assumed that the unit responds primarily to youth cases. However, in both 2016 and 2020 agents reported that *the majority of CyberScan cases involve adult complainants and respondents*<sup>22</sup> (CS2, CS7). In terms

<sup>&</sup>lt;sup>21</sup> MediaSmarts is a Canadian not-for-profit charitable organization for digital and media literacy.

<sup>&</sup>lt;sup>22</sup> It is not entirely clear why this is, it could be that youth are less likely to report the harms they experience, are more likely to access supports through family/school, or are less likely to contact CyberScan because the unit can only be

of the gender of complainants, agents in both 2016 and 2020 reported that most complainants are women/girls (CS2, CS3, CS7). Rough statistics kept by CyberScan from July 5th, 2018 to November 5th, 2020 show that 56% of complainants are female and 24% are male, with the remaining cases being unrecorded for various reasons (CS7). In terms of the gender of respondents, women/girls are also somewhat more likely to be respondents. Based on rough statistics kept by CyberScan from July 5th, 2018 to November 5th, 2020, 38% of respondents are female and around 26% are male, with the remaining cases being unrecorded for various reasons (CS7). Unfortunately, CyberScan does not currently keep statistics on the demographics of complainants and respondents beyond age and gender. An agent in 2020 expressed that such data should be collected "because with the cyberbullying you need to identify if there are target groups that are the victims of the cyberbullying. But unfortunately, the system is just not designed to capture that information" (CS7). Research shows that people who are LGBTQ+, Indigenous, racialized, and/or disabled can be disproportionately impacted by cyberbullying and nonconsensual intimate image distribution (Henry et al., 2017; Mishna & Van Wert, 2015); Therefore, CyberScan should consider keeping more detailed demographic data to ensure they are capturing the full picture of digital harm in Nova Scotia and are crafting appropriate resources and responses.

In terms of the relationship between complainants and respondents, in both 2016 and 2020 agents reported that most complainants and respondents are people known to each other rather than anonymous harassers. A 2016 agent explained that it was rare to receive a complaint where the respondent was unknown, "the vast majority of our cases are the peer-to-peer kind of cyberbullying where they are known to each other" (CS4). Agents in 2016 reported that many of their adult cases involve harm being committed in the context of the breakdown of an intimate relationship (CS1). As one 2016 agent explained, "I mean a lot of the adult ones we dealt with were domestic types in the sense of a separation or a break-up, some of them were even over child custody type of stuff, things like that. A lot of adult cases it was nonconsensual image distribution or [...] the threat of sending something like that out" (CS2). In 2020 agents explained that cases now seem to somewhat less often involve intimate partners and more often involve "adult neighbours, friends that have fallen out, etcetera" (CS7). The fact that most cases involve complainants and respondents who are known to each other provides important information for the kinds of responses and education that are required.

Recommendation #4: CyberScan should begin recording more detailed demographic data to ensure the unit understands, and appropriately responds to, those populations that are disproportionately impacted by cyberbullying and nonconsensual infimate image distribution.

contacted by phone and because youth require parental permission to speak with a CyberScan agent (See: Emotional support & information).

Giospanient correntonegui en vienal o la Lav aux hanage à l'Ottominium Document miles cett oursume to the Access la minimum 441

#### NUMBER OF CASES RESPONDED TO

During the 2 years and 4 months (September 2013-December 2015) that CyberScan was fully active under the original Cyber-safety Act, CyberScan staff responded to over 800 complaints (CS1). CyberScan staff described struggling to deal with the high call volumes they received during this time period: "[one of the most challenging parts of the job is dealing with] the sheer volume of cases, the very fast pace needed to keep up with it. So could be a good day where you'd have just maybe 10-12 calls a day or could be a day where you could receive 18 calls in one day" (CS1). Agents in 2020 reported responding to a much smaller number of cases under the Intimate Images and Cyber-protection Act, with 385 files opened between July 5<sup>th</sup>, 2018 and November 5<sup>th</sup>. 2020. CyberScan staff attributed the drop in cases as, in part, due to less public awareness of CyberScan than was the case when the unit was first created: "when [the new legislation] came out in 2018 it was more of a soft launch. There was no big media blitz like there was under the original legislation" (CS5). Another staff member likewise explained,

"It's a constant struggle trying to get the word out that we exist and that we are here as a resource. You know there are limited budgets for advertising I guess [...]. We target schools, make physical brochures, and then do outreach work sending out our website [...]. When the legislation was rolled out the communication department tried to [get the word out] and we had like videos made to be released on social media... but I don't know how popular that all has been...usually when [I ask how people heard about us] they'll say either the police have referred them [...] or it will be 'Oh a friend used you or I just researched online and came across your website.' And sometimes they will ask 'Are you a service for adults as well as youth?', so I've been asked that before and lots of other things" (CS7)

These comments reveal the need for further, or new types of, public outreach to spread the word that the CyberScan unit exists and that it has resources for both youth and adults. This, along with other issues in clearly communicating the resources CyberScan provides (See: <u>Communicatine CyberScan's role</u>), could be resulting in lower numbers of complaints to the unit. In the interest of creating wider public knowledge and use of the unit, it may also be worth considering renaming the CyberScan unit, as the name "CyberScan" does not clearly communicate anything about what the unit does to the average citizen. The unit might gain more immediate recognition if it were named something like "Cyberbullying Helpline", "Cyberbullying & Nonconsensual Intimate Image Distribution Helpline", or "Cyberbullying & Revenge Porn<sup>23</sup> Helpline".

Recommendation #5: Create a stronger public outreach campaign and online presence to ensure that the public is aware of what CyberScan is, who the unit can support, and what resources the unit offers.

Recommendation #6: Consider renaming "CyberScan" to ensure that the unit's name easily communicates the role of the unit to the public.

<sup>&</sup>lt;sup>23</sup> Although many scholars recommend avoiding the term "revenge porn", and instead using "nonconsensual intimate image distribution" or "nonconsensual pornography", it is worth considering which term is most likely to be familiar to the public and is most likely to be entered as a search term when seeking support. The United Kingdom, for instance, has selected "Revenge Porn Helpline" as the name for their support line for victims of nonconsensual intimate image distribution.

## TYPES OF DIGITAL HARM

Based on rough data<sup>24</sup> kept by CyberScan from July 5<sup>th</sup>, 2018 to November 5<sup>th</sup>, 2020, an agent reported that approximately 70% of the cases CyberScan responded to were cyberbullying cases, 7% of cases included both cyberbullying and nonconsensual intimate image distribution, 5% of cases included only nonconsensual distribution, and the remaining cases were not categorized because they were referred from other agencies (CS7). In terms of the types of cyberbullying that occurred during this same period, rough estimates indicate that approximately 29% of cyberbullying cases included "nasty comments and name calling"; 20% involved "threats, intimidation, or menacing comments": 17% involved "false allegations": 13% involved "impersonation accounts"; and 12% involved "unwanted contact and harassment"<sup>25</sup> (CS7).

In addition to noting various types of acts such as "name-calling", CyberScan should consider also documenting the types of discrimination that likely underly many of their cases. *When simply logging types of harm such as "name calling" without noting whether it was, for instance, homophobic, sexist, or racist name calling, trends in systemic discrimination—or what Mishna & Van Wert (2015) call "bias-based cyberbullying"—cannot be revealed or addressed. As discussed further in the below section on education (See: Educational presentations) and the above section on restorative approaches (See: Taking a restorative approach?), CyberScan should ensure that their work is alive to the discriminatory beliefs that often underly the most harmful acts of cyberbullying and nonconsensual distribution. If CyberScan began to track for forms of discrimination they could, for instance, find a pattern of homophobic bullying among youth and use this as a catalyst to work with schools on cocreating a plan to counter homophobia.* 

The rough estimates above demonstrate that the CyberScan unit responds to a variety of digital harms. Some examples of specific acts that CyberScan interviewees described responding to are listed below.

Agents in 2016 provided the following examples of types of cases they respond to:

- An ex-partner distributing intimate images without consent following a breakup (CS2).
- A young person nonconsensually distributing intimate images of a friend (CS2).
- An ex-partner creating fake social media accounts to repeatedly contact and threaten their ex-partner (CS2).
- An ex-partner using social media to continually post offensive comments about their expartner (CS4).
- A young person posting derogatory comments about a peer on social media that other young people use as fodder for further online and offline bullying (CS1).
- A young person screenshotting a private conversation and sharing the screenshot with others leading to widespread online and offline bullying (CS1).
- Teen girls sharing private information about a friend's sex life on social media (CS2, CS1).

<sup>&</sup>lt;sup>24</sup> The staff member reporting this data stated that all percentages should be interpreted as rough estimates as the data is inputted in a somewhat informal manner and there are sometimes holes/overlaps in data recording (CS7).

<sup>&</sup>lt;sup>25</sup> These rough percentages do not add up to 100% because some cases are referred from external agencies and are not coded in the system and because a single case can be coded as including multiple types of cyberbullying.

- Posting derogatory comments about individual community members on neighbourhood Facebook groups and encouraging others in the neighbourhood to pile-on by making fun of or bullying the targeted person (CS4).
- Young people creating fake social media profiles of their peers that are used to make fun
  of them (CS2).

Agents in 2020 provided the following examples of types of cases they respond to:

- Posting "nasty name-calling" about someone on social media (CS5).
- A male partner threatening to post intimate images of their female partner if they breakup with them (CS5).
- An ex-husband nonconsensually distributing intimate images of his ex-wife to try to undermine her reputation during a custody hearing (CS5).
- A young person making a social media account under their school's name (e.g. "Citadel High Confessions") to post rumours about or make fun of individual students (CS5).
- Parents screenshotting bullying messages sent to their child and posting the screenshot on social media to encourage adults to publicly shame the bullying child (CS5).
- Young people creating a shared group chat for their class but leaving out select peers that are made fun of in the chat (CS5).
- Posting private information, images, and/or rumours about someone on public websites designed specifically for anonymous rumour posting and reputational harm (CS6).

These examples help to further demonstrate the various types of cases that CyberScan is tasked with responding to.

Recommendation #7: Begin Iracking forms of systemic discrimination reported to CyberScan to ensure the unit's work at the individual and systems-level addresses relevant issues of systemic discrimination.

# CYBERSCAN'S RELATIONSHIP TO CIVIL & CRIMINAL JUSTICE PROCESSES

Although the CyberScan unit responds to almost all cases through informal responses, CyberScan sometimes helps complainants navigate civil or criminal law processes. The first subsection below outlines CyberScan's relationship to civil law processes and the ways this has changed since CyberScan's inception. The second subsection outlines the unit's relationship to the criminal justice system. The final subsection discusses how the professional backgrounds and training experiences of some CyberScan agents create additional ties to traditional legal responses.

# USE OF CIVIL COURT ORDERS

Under the original *Cyber-safety Act* (2013), CyberScan was able to apply for Cyberbullying Prevention Orders in those cases where informal responses were unsuccessful. *However, even when CyberScan had this power, the vast majority of the unit's cases were responded to without recourse to civil court orders.* CyberScan agents in 2016 reported that the unit used this civil law

option in only two<sup>26</sup> cases during the life of the *Cyber-safety Act* (though some members of the public also applied independently for Cyber *Protection* Orders under this legislation) (CS2; CS4). One 2016 agent asserted that CyberScan only applied for court orders in the very few cases where informal responses or warning letters were deemed unsuccessful. In these cases, complainants were deemed to be experiencing "extreme stress and extreme anxiety" and the bullying/harassment was ongoing or had escalated despite informal interventions (CS4). While court orders were rarely used by CyberScan even under the sweeping *Cyber-safety Act*, it is important to note, as privacy lawyer David Fraser has argued, that some CyberScan agents may have used the *threat* of court orders in a manner that resulted in undue limitations on free expression (Fraser, 2017) (See: <u>History of CyberScan</u>).

Under the current Intimate Images and Cyber-protection Act (2017), CyberScan agents can no longer send formal warning letters regarding potential legal action and can no longer apply for court orders on behalf of complainants. Complainants must now navigate and pay for applications for court orders (i.e. Cyber Protection Orders) on their own, which can be a cumbersome and costly process. As one agent described:

"It's a lot of pressure for somebody to have to go fill out all those forms. If someone is harassing you or whatever, think of all the stress you already have in life, whatever is going on with kids, financially, relationship breakdown, and now maybe you don't have the capacity electronically to do this, or you don't have the money, or a vehicle to get from point a to point b for the courthouse. And now you're responsible to download all this paperwork, fill it out appropriately, and then file it, and then there is a cost<sup>27</sup> to that too" (CS4).

When CyberScan staff were interviewed for this report in November of 2020, they had not supported a single complainant that chose to apply for a court order under the current legislation. Additionally, they knew of only one person who had applied for a court order on their own (this person had not contacted CyberScan before proceeding and the unit only learned of the case through media coverage) (CS5, CS6). Thus, under the current legislation, civil law remedies are even more rarely used and CyberScan has very little relationship to civil law aside from the ability to explain the application process for court orders to complainants that wish to apply on their own. One agent explained the limited role CyberScan now plays saying, "[if a complainant] wants to know a lot about the Cyber Protection Order process we will send them links about what the affidavit process looks like [...] and a link to the legislation. [...] But again, it doesn't have anything really to do with us... it's a separate process when you are applying to court" (CS5). While CyberScan agents have not yet supported a complainant that has followed through with the court order process, the CyberScan website does include a detailed document titled <u>"What you Need to Know about the Intimate Images and Cyber-protection Act"</u> that could be used by those

<sup>&</sup>lt;sup>26</sup> Minister of Justice Mark Furey has stated that under the original legislation "CyberScan investigated over 800 cases and, of those, ten cases went to court" (Nova Scotia, Legislative Assembly, *Hansard*, 63<sup>rd</sup> Leg, 1<sup>st</sup> Sess, No 27 (12 October 2017) at 1166). It is unclear why exactly Furey cites 10 cases and CyberScan agents cite two, but it is possible that the ten cases mentioned include both those applied for by CyberScan and those applied for by the public independent of CyberScan.

<sup>&</sup>lt;sup>27</sup> It costs approximately \$250 to apply, which can be waived for people below a certain income level who apply for a fee waiver. However, this cost, which is already inaccessible to some, will be much higher if the complainant requires a lawyer.

applying on their own. This document explains the ways a Cyber Protection Order could be useful in terms of having images or content ordered to be removed, potentially receiving monetary damages, forbidding the respondent from contacting the complainant, or ordering disputeresolution services. This document also explains that the process can be challenging and costly. Although this document is clearly written and could be useful to complainants, the amount of detail provided within it also acts to reveal just how complex and inaccessible the court process can be for the average citizen.

CyberScan agents expressed that the limited support they can now provide for applying for court orders acts as a significant barrier to responding to those rare cases where informal supports are insufficient. One 2020 agent explained that, under the current legislation. CyberScan has responded to about 7 cases in which they believed that informal processes had not resolved the matter and that a complainant might want to apply for a Cyber Protection Order (CS7); However, in each of these cases complainants reportedly did not to move forward with the application because "the court process was too onerous for them to actually want to pursue it" (CS7). The court process was seen as especially onerous in rare cases where the complainant is unaware of the identity of the cyberbully; In such cases, the process involves first applying to reveal the respondent's identity before applying for a court order (CS5; CS7). Therefore, agents in 2020 expressed that the current legislation should be updated to provide more support for complainants in those rare cases where. despite informal responses, harm is severe and ongoing (CS5; CS6; CS7). David Fraser, the privacy lawyer who argued that the original legislation was overly broad and violated the rights of accused people, has also expressed concern that the new legislation may have "[swung] the pendulum a little bit too far" by leaving victims to fend for themselves in court or hire a lawyer at significant cost (Palmeter, 2017).

In addition to the challenges of accessing civil remedies, CyherScan agents explained that there are several other reasons that complainants are often uninterested in engaging civil law. For instance, agents explained that there is a risk that going to court will simply bring more attention to the case and thereby result in more people in the community expressing opinions about or bullying the complainant (CS5, CS3, CS7). Although anonymity can be granted to complainants in some cases and is automatically applied to those under 19, in those cases where anonymity is not promised the complainant may worry that a court process will only bring more attention to the rumours, private information, and/or discriminatory content being disseminated about them (CS7). One agent explained that, even if anonymity is granted, complainants in small communities often worry that their identity could still easily be revealed by word of mouth (CS5). As a 2016 agent put it:

"Complainants definitely [want to keep it informal], especially in small communities. You know, if you can handle this here... it'll go away here. [If you take it to court] the problem can get bigger, there's a fear of further exposure, there's fear of public display, of it becoming a bigger thing than it maybe needed to, you know. Certainly a lot of it was the private sexual information or images for females, especially. So the bigger it may have become, was certainly a problem for them. We did it the right way. I have no doubt about it... with that informal resolution. [...] It's the most efficient way to deal with the social media problem that we're facing for sure." (CS3)

This agent explained that many complainants see a court process as counterproductive, as it may result in additional and extended attention being given to their nonconsensually distributed intimate images or to the harmful comments being made about them through cyberbullying behaviour. This agent explained that this might be especially the case for female complainants who have had intimate images or private information/rumours about their sexual lives digitally disseminated. Another reason complainants may not proceed with a court order is that applying for an order is a slow process and the damage may already be done by the time an order can be made (CS7). While civil law remedies have been utilized in a few cases where informal responses were deemed inadequate, it seems that civil law remedies are rarely more appealing than the informal options offered by CyberScan. Therefore, in addition to considering ways to make civil options more accessible, it is important to adequately resource the CyberScan unit and ensure that the public is aware of the informal options the unit offers.

Recommendation #8: Consider providing additional supports for complainants in those rare cases where civil law remedies are pursued.

Recommendation #9: The government of Nava Scatia should continue to fund CyberScan's resources for informal responses as court orders are rarely used and have several limitations. The government should consider whether CyberScan is able to adequately provide the important informal supports they offer with their current number of staff.

## RELATIONSHIP TO CRIMINAL RESPONSES

The CyberScan unit can respond both to acts that rise to a criminal level (e.g. cyberbullying cases that amount to criminal harassment and cases of nonconsensual intimate image distribution) and acts that do not rise to a criminal level. While the unit is sometimes misunderstood as working only to respond to cases that would otherwise not qualify for government response, the CyberScan unit also plays an important role as an alternative option to the often blunt and slow criminal justice process. In Murray Segal's (2015) independent review of the Rehtaeh Parsons case, he speaks to CyberScan's role as a necessary alternative option:

"The criminal prosecution of individuals should not be the be-all and end-all of solutions. While there will always and should always be a place for the traditional police investigation and criminal prosecutions, which can be valuable tools for reducing crime, we should not lose sight of the fact that they are only one set of tools. We must accept their limitations and embrace alternative solutions. [...] In particular, I think of the CyberScan initiative [...]. This unit [...] will investigate allegations of cyberbullying and intervene if warranted. They have a host of measures at their disposal to stop bullying while, at the same time, raising awareness among cyberbullies and the public." (p. 41)

Evidencing the limitations of typical criminal justice responses and the need for various "sets of tools" to respond to digital harms, CyberScan agents report that most complainants who contact them are interested in accessing informal supports to resolve even criminal level harms in more expedient and victim-centred ways (CS2; CS5; CS6). As discussed further below (See: Most

<u>common responses</u>), most complainants are more interested in receiving expedient technological and emotional/informational support than they are in having the respondent investigated or punished. Considering this, it is important that CyberScan is understood not only as a resource for cases that do not rise to the criminal level, but also as an in-demand alternative response to criminal level cases.

CyberScan agents seem to vary in the extent to which they promote CyberScan as an alternative option that is available even in cases that rise to a criminal level. At least two CyberScan agents expressed strongly encouraging complainants with criminal level cases to report to police. For instance, an agent in 2016 explained that they tell victims of nonconsensual intimate image distribution that "it's a federal offence and to contact their local policing agency" (CS1). An agent in 2020 described that, although they recognize many complainants do not wish to pursue a criminal response, they still encourage complainants to go to the police if their case involves potentially criminal acts: "obviously if there is a criminal element I will say 'These are criminal offences', and though we have a role as well I will refer them to police, like say 'You really need to go back to the police or make a report to the police" (CS7). These agents seem to imply that complainants *should* pursue a criminal response when possible, despite the fact that most of the complainants the unit supports are more interested in accessing alternative supports. Recognizing the many reasons particular complainants might have for preferring alterative responses, many other CyberScan agents explained that they describe the various support options available to complainants without implying that complainants should go to the police or that the criminal justice process is necessarily the best option. Although agents seem to vary in the extent to which they encourage complainants to make formal complainants to police, all agents recognized that this option was not desired by most complainants. As an agent in 2016 described, complainants often see formal criminal justice approaches as unappealing and are more interested in the expedient and informal supports CyberScan can provide:

"A victim of cyberbullying... a victim of any of this...they just want it to stop. [...] I find they don't want to go to court and, you know, keep the attention on this for a long time. No, they want help to get the image down or the content down and get that deleted so that it's not posted again and it stops spreading to others. They want it to stop so they can get on with their lives. And we were able to deliver that for the majority of [victims]. And we'd be able to it quickly." (CS2)

Agents explained that complainants generally do not wish to extend the time and attention paid to the harm they experienced through a criminal process and, when told they can access supports without requiring a formal criminal process, most complainants are eager to address the case informally with CyberScan. One 2020 agent explained that *some complainants also prefer informal responses because they do not wish to criminalize the respondent*. Especially in cases where a complainant is or was in a close relationship with the respondent, they often want the respondent to understand the harm they are causing but do not want the respondent criminalized (CS5). This agent provides the example of a complainant who had her intimate image distributed without consent by an ex-partner that was struggling with alcoholism. The complainant wanted the respondent to know that what they did was harmful and to get support to deal with their use of alcohol, but they did not see a criminal response as helpful (CS5). This agent explained that, when considering what response will be most helpful, you have to ask "Is it best to charge them criminally with that? Or is it best to look at the particular incident and kind of learn from it? And especially if the person is remorseful and takes responsibility for it and we can kind of move forward ... it's just so much better to go ahead with it that way" (CS5). Echoing CyberScan agents' experiences with complainants in many ways, research on cyberbullying and nonconsensual distribution has also found that legal approaches can be unappealing as they are often lengthy and can extend the life of a conflict (which can be particularly damaging in youth cases), they're largely offender-focused and not responsive to particular victim and community needs, they're punitive-focused and not necessarily designed to help respondent's meaningfully learn and change, and they can result in revictimization due to officials, such as police officers, that may engage in victim blaming/shaming<sup>28</sup> (Choo, 2015; Dodge & Lockhart, 2021; Powell & Henry, 2017; Shariff & DeMartini, 2015).

In cases where complainants do decide to report to police, CyberScan sometimes stays involved with the file in a victim support role (i.e. emotional/informational support and help navigating the criminal justice system). An agent in 2016 described performing this role in a case involving nonconsensual intimate image distribution: "The police [...] moved forward with criminal charges and then we were kind of a resource or a [...] friend I guess. So the victim she did keep in contact with one of the [CyberScan agents] and was able to get advice that she needed [...] and, even though we weren't active in the investigation because it was a policing file, she still knew that we were here" (CS1). An agent in 2020 explained that a similar victim support role continues in CyberScan's current form: "We do work in conjunction with police, you know if there is an ongoing police investigation we will say, 'What can we do to assist? What is our role here? How can we help?' It might just be a matter of being the liaison because the complainant is frustrated that they aren't getting any updates and we can say 'Who is the officer?' and just trying to help in whatever way we can" (CS7). These agents described filling some of the victim support needs that are often not adequately provided by the criminal justice system itself. In this way, CyberScan acts as both an alternative to criminal justice responses and as a support to fill gaps in typical criminal justice responses.

CyberScan agents also described sometimes working in a kind of "tech support" role for police officers who often do not have the full technological know-how to respond to cases involving digital harms. When asked if, in their experience, police officers are equipped to respond to cases involving digital technology, one agent in 2016 replied:

"The difficulty is, in my experience, that police officers are supposed to be [...] experts if you will in every area and [...] that's difficult unless you have special units or you have ongoing training. [...] So a lot of police officers don't have the technical background or understand social media and [...] a lot of the frontline members don't know how to preserve accounts for example on Facebook. They don't know how to preserve the evidence legally in order to get an order from a court to get the IP address or whatever. So we educate them for sure, all the time too. They're becoming better with it, because we've been working with them a lot. And we'll assist them if they just want information on 'How do I do this

<sup>&</sup>lt;sup>28</sup> A recent example of criminal justice responses resulting in victim blaming can be seen in the case of a woman who reported several cases of nonconsensual intimate image distribution perpetrated against Indigenous women to the Nova Scotia RCMP. She reports that she felt the RCMP response engaged in victim blaming by responding that she should tell her friends never to share intimate photos with anyone. This woman states: "We don't need a lecture. It's not our fault that these men put these photos on these websites without our consent" (Reynolds, 2021).

with Twitter?' or whatever, then we'll walk them through that stuff. [...] A lot of the information is available online now through those social media sites, but again it's just very difficult for a person to understand all of these things [...]" (CS2).

Another agent in 2016 similarly explained, "I think that my experience tells me that [police officers] are terribly under... not aware of the situation of social media. [...] I personally spoke to at least twenty police officers who said to me 'What's this [social media] all about? What am I supposed to do? I don't know what to do. Can you help me? I'm lost here.' That was often the response that I got from the police officers, both the RCMP and the municipal police" (CS3). This agent also explained that some complainants come to CyberScan saying that frontline police officers were completely unable or unwilling to provide assistance because they didn't understand the nature of the digital harm being reported (CS3). One interviewee in 2020 confirmed that CyberScan is still sometimes involved in supporting police officers to understand many aspects of responding to cases involving digital technology (CS7).

Recommendation #10: CyberScan's communications with individual complainants and with the general public should explain that the unit is both a resource for dealing with harms that do not rise to the criminal level and an in-demand alternative to criminal justice responses.

Recommendation #11. CyberScan should be resourced at a level that recognizes the variety of ways that agents work to address gaps in the traditional criminal justice response.

#### TRAINING & PROFESSIONAL BACKGROUND

*CyberScan staff mainly have professional backgrounds in policing, corrections, and government enforcement roles.* Of the four CyberScan staff interviewed in 2016, one had a professional background in government enforcement, two were ex-police officers, and one had a background in corrections. With CyberScan's mandate being to respond primarily through informal, restorative, and educational approaches, it is surprising that hiring has focused narrowly on those with more traditional criminal justice and enforcement backgrounds. In 2020, CyberScan staff also had professional backgrounds related to policing, corrections, and enforcement; However, these staff described having worked in roles that were more focused on justice advocacy or victim support within these professions, and one staff member also had considerable background experience working with digital forms of harm. Therefore, while there are still gaps in the skillsets that would be needed to provide robust restorative or educational responses, CyberScan staff in 2020 seemed to have more experience to draw from in terms of the support aspect that makes up a large portion of CyberScan's work.

Considering that CyberScan's role is increasingly focused on providing emotional support, assistance with reporting/removing harmful digital content, and providing educational presentations, future hiring choices should consider what gaps in knowledge might be filled by hiring those outside of the worlds of policing, corrections, and enforcement. For example, although education makes up a significant portion of CyberScan's role (See: Educational presentations), CyberScan staff do not feel they have expertise in this area (CS5, CS6). Future hiring should consider diversifying the backgrounds of staff by adding, for instance, those with experience in youth education, counselling, tech support, and restorative approaches. As one of the restorative approaches experts commented, "I think [CyberScan] did in some ways hire people interested in different approaches to public safety... but certainly there wasn't a lot of balance on the team in terms of educators, community organizers, facilitators or people who have worked in this [restorative] way. You could imagine hiring kind of a balance of people that could have brought their various skills and helped each other" (RA2). Diverse skillsets could only be a positive addition in terms of CyberScan's mandate to "try to think outside the box [of typical legal approaches] to assist Nova Scotians" (CS6).

In terms of the training provided to CyberScan staff, in both 2016 and 2020 agents described receiving police training courses in online investigation techniques and forensic interviewing. Again, considering their mandate to primarily respond through victim support, restorative approaches, and educational presentations, it is surprising that staff are not provided training in areas such as restorative approaches, best practices for supporting people in distress/crisis, or best practices in educational engagement. Additionally, as CyberScan responds to many cases that include some element of sexual violence (e.g. nonconsensual intimate image distribution or sexualized cyberbullying) or domestic violence (e.g. threats to distribute intimate images if a person ends an abusive relationship or campaigns of online rumour spreading in the aftermath of a breakup). CyberScan agents should receive specific training in how to support victims of sexual and domestic violence. Although CyberScan staff expressed that they generally felt equipped to respond to cases based on their backgrounds in policing, corrections, and enforcement, it is worth considering how responses could be improved by providing training in areas such as supporting someone in distress/crisis, supporting victims of sexual and domestic violence, and providing education to youth. In terms of acting on the promise to provide a restorative approach (See: Taking a restorative approach?), the restorative approaches experts interviewed for this report were adamant that, to truly work restoratively, simply providing training sessions to CyberScan staff will not be enough. As one of these experts stated, "we cannot teach a restorative approach through a one-day workshop. [....] we have to set up the system and create relationships to be able to work with people who want to work [restoratively]" (RA1). This interviewee felt that government leaders need to refocus on the restorative approach that was imagined during the envisioning of CyberScan and support CyberScan staff in taking this approach (RA1).

> Recommendation #12: Future hiring, training, and resourcing for the CyberScan unit should focus an filling gaps in terms of the unit's ability to robustly support people in distress/crisis, support victims of sexual and domestic violence, provide education to youth, provide technological support, and respond restoratively.

Dissument common and in view of la Lin and canada it Tollormolour Disconont released a vision fo the Access to intermenting with

# MOST COMMON RESPONSES

From its inception, CyberScan has responded to the majority of cases using what agents refer to as "informal" approaches. As detailed in the subsections below, the most common responses provided by CyberScan include helping complainants to remove/report nonconsensually posted intimate images or cyberbullying content from social media platforms/websites and providing emotional/informational support to complainants (CS7). Much more rarely, CyberScan staff contact the respondent to attempt to have them remove images/posts and stop further bullying by explaining the harm they are causing and/or describing the potential legal impacts of their actions. In very few cases, CyberScan staff assist complainants with navigating legal options (See: CyberScan's relationship to civil & criminal justice processes). CyberScan staff explained that, above all, their approach is based on meeting the stated needs of complainants: "The main thing when it comes to complainants that call in is [to ask] 'What do you want to see happen? What is it that you are looking for?' Because we have lots of options, but it's about letting them choose, because this is their file" (CS6).

## IMAGE/CONTENT TAKEDOWN AND TECHNOLOGICAL KNOW-HOW

Agents in both 2016 and 2020 shared that helping complainants to report/remove harmful social media posts and website content is the most common response they provide. A 2016 agent asserted that "99.9% of [complaints] just want the cyberbullying to stop and the comments to come down" (CS4). Even in cases of nonconsensual intimate image distribution, in which complainants have the clear option to report to police, agents explained that most complainants "just want it to stop, they want the image deleted from the other persons device, that's mainly it. [...] Like if a woman is calling and saying, 'I don't want him contacted, I just want that image taken off the web', then we will go on there and find out how to take the image down and offer as much support as we can with that" (CS5). CyberScan's role in providing technological support is extremely important as agents consistently explained that the main concern of most complainants is to have harmful content removed. For example, a 2016 agent described a case in which a woman's ex-boyfriend had posted offensive claims about her online and it wasn't until this content was removed that she felt she could go out in public in her small community again and "put her head up and get on with her life" (CS3).

CyberScan can provide technological supports by helping complainants to navigate standard avenues for content reporting/removal (e.g. reporting mechanisms on various social media platforms or requests to delist nonconsensually posted intimate images from Google search results) or by using their "established strong networks [...] with social networks like Twitter and Facebook" to expediate this process (CS5). In some cases, content is removed by contacting the respondent to request voluntary removal. As expediency in removing or stopping the spread of cyberbullying content and/or nonconsensually distributed intimate images is often top of mind for victims (Choo, 2015; Segal, 2015; Shariff & DeMartini, 2015), it is vital to offer this kind of support for content reporting and removal. In Murray Segal's (2015) review of the response to the Rehtaeh Parsons case, he praises CyberScan's approach in this regard as one of "the most novel and directly responsive solutions to what was arguably the most time-critical aspect of Rehtaeh's torment: getting ahead of the damaging photograph that was circulating like wild-fire among her

peers" (p. 116). An Agent in 2016 expressed that, in cases of nonconsensual intimate image distribution, they were often able to have posts removed quite quickly: "we tell victims, 'we will help you try to get these photos back and we will do it as quickly and as discretely as possible'. [...] Our response time is very quick when we do that kind of stuff' (CS2).

CyberScan agents explained that some platforms and websites are very responsive to requests for removal of harmful content; However, content removal is not always straight forward or expedient. Agents explained that certain platforms/websites can be more challenging to work with and certain kinds of content can be more challenging to address. An agent in 2020 explained that, even when working with the dominant social media platforms that can be quite responsive, issues such as fake accounts can be more difficult to expediently remove: "[fake] Instagram accounts seem to be a big thing right now [...] and trying to get it taken down is not easy, it's not going well" (CS6). Websites such as "The Dirty", that are devoted solely to posting rumours and bullying/harassing content, can also be much more difficult to deal with. As one agent in 2020 explained, such websites will often refuse to remove offensive content about an individual; However, for those websites based in the United States, CyberScan has had success with having *images* of complainants removed through the use of the Digital Millennium Copyright Act (1998) (CS6). Agents also described that, although they are certainly able to assist more quickly than through formal legal channels, content removal is still sometimes a slower process than they would like it to be. An agent in 2016 explained that "[One of the most challenging aspects of the job] is our inability to have social media companies provide us the closure that we want instantly. [...] it's a challenge to get an immediate response" (CS3). An agent in 2020 likewise explained that they "wish there was a quicker way to get posts taken down" (CS5). Although content cannot always be fully removed or expediently removed, agents described being at least partially successful in most cases and reported that complainants are usually very grateful for any support that can be provided in this regard.

*CyberScan's knowledge of the most problematic websites/platforms to work with and the most challenging types of content to remove should be used to inform federal initiatives<sup>29</sup> that are currently investigating ways to make social media platforms and websites more responsive to requests for removal of harmful content (Khoo, 2021).* Changes already implemented by some social media companies and search engines have shown promise in terms of making content removal easier and more expedient in some cases. Especially regarding nonconsensual intimate image distribution, many social media platforms and search engines (e.g. Google and Bing) have created somewhat more effective reporting options due to activist pressure (Online Removal Guide, 2021). Defining what content should and should not be removed can sometimes be a challenging balance between considerations of harms caused versus freedom of expression (See: Khoo, 2021); However, websites and social media platforms should be able to at least decrease response times to clearly criminal content, such as nonconsensually posted intimate images (Crofts & Lievens, 2018; Khoo, 2021).

While social media platforms and websites are often responsible for slow responses to requests for content removal, an agent in 2020 also described how CyberScan's response can sometimes slow down this process. CyberScan only accepts calls during regular business hours Monday to Friday, which means complainants who call in the evening, on a weekend, or on a holiday will not

<sup>&</sup>lt;sup>29</sup> https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html#a3

receive supports for several hours or days: "you know you get the call [from the complainant], it's not maybe until the next day that you [can respond]. [...] technology moves so quick that the damage is already done. [...] then even if you report it, it might take a week to be taken down [...]. So it's just that I wish there was a way that... some of the posts are just so harmful to people, even just talking about rumours [...] by the time they ever get shutdown the damage is already done" (CS6). CyberScan's role in slow response times could be addressed by expanding the unit's hours and linking to do-it-vourself resources that help individuals learn how to report bullying posts or nonconsensually shared intimate images on various platforms. Although not all complainants will be able to navigate reporting on their own, links to these resources would certainly be useful for a portion of complainants that are struggling with time-sensitive needs. CyberScan's website should share links to resources such as Google's form for reporting intimate images shared without consent<sup>30</sup> and NeedHelpNow.ca's<sup>31</sup> instructions on how to report content on Snapchat, Instagram, YouTube, or a peer's phone. International resources, such as Australia's eSafety Commissioner<sup>32</sup> website, the United Kingdom's Childline<sup>33</sup> website, and the Cyber Civil Right's Initiative<sup>34</sup> in the US, provide additional resources on how to report cyberbullying or nonconsensual distribution on platforms such as Twitter, TikTok, WhatsApp, and more. CyberScan could provide links to this kind of do-it-yourself reporting information while also encouraging complainants to contact the support line for additional help during operating hours.

As described above (See: <u>Communicating CyberScan's role</u>), CyberScan's website and resources could do a better job of explaining the supports they provide in terms of content reporting and removal. The CyberScan website should highlight this service and provide reassuring messaging to complainants that may be feeling hopeless. As shown in the below image, the UK's Revenge Porn Helpline<sup>35</sup> provides a useful example of the kind of reassuring messaging that should accompany reporting/removal resources:

#### What happens if I find a result?

If you do find a result and there is an intimate image or video shared without your consent, we're here to help you.

- Firstly, don't panic. That's easier said than done, but we can help. You're not alone in dealing with this.
- Screenshot the page where it has been posted and save it. This is evidence if you decide to report to the police. You can do this by
  calling the police non-emergency number 101; you'll need to give brief details to a call handler and an appropriate officer should return
  your call.
- Contact the Helpline. We are able to help you to report and remove the content. Whilst we cannot guarantee it will be removed, we do
  hold a very good takedown success rate and we are very persistent and determined.
- Provide us with links. We will ask you to copy and paste the URL and send us the links to the content; if there are other images or videos on the page, we may have to ask you to confirm which images are of you.

It's important to note the reassuring tone of the above messaging provided by the Revenge Porn Helpline. Although guarantees about image removal cannot be made, the messaging ensures victims that there are supportive resources available to them and that there is hope. Another

<sup>&</sup>lt;sup>30</sup> https://support.google.com/blogger/answer/7540088?hl=en

<sup>&</sup>lt;sup>31</sup> Needhelpnow has useful tech know-how resources, however it should be noted that some of their materials have been found to engage in victim blaming/shaming or provide an overemphasis on criminal law: https://needhelpnow.ca/app/en/#

<sup>32</sup> https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/report-to-social-media-website

<sup>33</sup> https://www.childline.org.uk/info-advice/bullying-abuse-safety/types-bullying/bullying-social-media/

<sup>34</sup> https://www.cybercivilrights.org/online-removal/

<sup>35</sup> https://revengepornhelpline.org.uk/

example of how to provide tips for reporting along with reassuring messaging can be seen in the below MediaSmarts resource for Canadian youth:



Unlike some materials for youth that aggravate anxiety through worst-case-scenario assertions that nonconsensually distributed intimate images will irreparably impact a victim's reputation and future job and school prospects (Angelides, 2013; Dodge, 2021), this resource provides reassurance that there are supports and tools available to alleviate and heal some of the harms being experienced and that a youth does not need to panic. By linking to resources such as these, CyberScan could easily provide more expedient technological support and reassurance to complainants. However, online guides should not replace the ability to get one-on-one support from a CyberScan agent, as several agents asserted that the human connection with complainants can be healing and that many Nova Scotians struggle to understand do-it-yourself instructions due to low levels of technological know-how. One-on-one support also allows agents to determine and support other technological needs. For example, CyberScan agents often provide complainants with additional technological know-how such as explaining that unwanted contacts can be deleted or blocked on social media platforms: "part of the job is doing research on what the community guidelines are on say Facebook or something like that and letting the person know about blocking features and deleting, because some people surprisingly still don't know about some of those options, if something happens they don't know you can delete the person or block them" (CS5).

Recommendation #13: CyberScan's knowledge of the most problematic platforms/websites to work with and the most challenging types of content to remove should be used to inform federal initiatives investigating ways to make platforms/websites more responsive to takedown requests.

Recommendation #14: Due to the often time-sensitive nature of digital harms, CyberScan should consider expanding their operating hours and linking to do-it-yourself content reporting/removal resources to ensure that complainants can access immediate technological support.

### EMOTIONAL SUPPORT & INFORMATION

Emotional support is the second most common response CyberScan provides. As an agent in 2020 described, it can be a comforting and validating experience for complainants to simply speak with someone who has knowledge of cyberbullying and nonconsensual distribution and can assure complainants that they are not alone and are not at fault for having been victimized:

"what I hear from a lot of complainants is that it was nice just to have someone to actually talk to, and that made a big difference. And just to hear that it's not their fault. Because sometimes they are so upset when they are talking to you, and so when we tell them you know 'It's not your fault, we get calls like this all the time', a lot of feedback I always hear is 'It was so nice to just feel like I wasn't judged, I just felt so stupid that I allowed this to happen, and just knowing that someone...'. And I tell them, 'Well, this is why this unit was actually created, because this has caused so many problems for people'" (CS5).

As this agent described, it can be a powerful step in healing to have someone listen to your struggle without judgement and ensure you that you are not alone in this experience. CyberScan agents feel that their experience working in the unit makes them well positioned to comfort complainants as they can "provide understanding" of the types of harms being experienced and provide information on the supports that have been helpful for other victims (CS5). While in many cases agents provide emotional support in combination with the technological supports described above, agents also explained that in some cases emotional support is the sole support requested. As a 2020 agent described, complainants are sometimes dealing with online public shaming that is already widespread and, although little can be done to mitigate the spread, CyberScan can still provide emotional support: "[sometimes the complainant] is devastated you know, but later they will thank me and say, 'even talking to someone who knows what it's like and has that experience helped a lot" (CS5). For complainants requiring additional emotional support, CyberScan agents also provide information on counselling and mental health supports in the community. As a 2016 agent explained, in several cases CyberScan has helped parents to find additional mental health support services for a child experiencing digital harms: "there are a lot of parents in the province that [...] don't know how to use a computer, so they don't even know who to call. If they ask for information for further supports, we will take whatever time is necessary do the research we need to do to provide them with the information they request" (CS2).

While it is a positive finding that CyberScan provides needed emotional support to complainants, there are also several ways in which this support could be improved and made more accessible to all complainants. As an agent in 2016 described, it can sometimes be challenging for CyberScan staff to deal with the range of intense emotions that complainants might be dealing with when they contact CyberScan:

"a lot of times [...] emotions were very high when you get those types of phone calls. [...] I would just try to listen to that person and let them know that there's somebody on the other end that would do whatever they can to help. And if there's something that we couldn't do, then to maybe give them other resources, tools they could use... but generally it was important to be there and listen and try to calm that person down and obviously help them the best way that we could. [...] you're dealing with people with mental health problems at times and then obviously the people that are very much in crisis" (CS1).

As CyberScan staff are sometimes tasked with responding to people who are in serious emotional distress or crisis at the time of their call, CyberScan agents should receive training in best practices for supporting those in distress/crisis (See recommendation above: Training & professional background). As CyberScan deals with many cases involving aspects of sexual violence or domestic violence, agents should also receive training in best practices for supporting these victims (See recommendation above: Training & professional background). As CyberScan deals with many cases involving aspects of sexual violence or domestic violence, agents should also receive training in best practices for supporting these victims (See recommendation above: Training & professional background). Sexual violence support training is important to ensure, for example, that CyberScan agents do not engage in the kind of victim blaming and shaming that some victims of nonconsensual intimate image distribution have experienced when reporting to police (Henry et al., 2018) and that is often present in educational responses to youth (See: Education regarding nonconsensual intimate image distribution).

*CyberScan's ability to emotionally support complainants is also limited by their hours of operation.* While agents described some callers as being in distress/crisis and in need of immediate emotional support, the CyberScan phoneline is only open to take calls on weekdays during normal business hours. As one interviewee in 2016 explained, these limited hours of operation often make it difficult to connect with clients in need of support:

"generally [complainants] are at work or school from 8:30 to 4:30, so I changed my hours to 8 to 4 and I kind of stay in the office through lunch hours so that I can be more accessible [...]. And then obviously you want to try to hit people first thing in the morning so getting that phone call to them at 8 o'clock as opposed to 8:30 when they already left for work or school. I provide people my cellphone number so that they can access me at home if they didn't want to contact me while they're at work or if they don't get home until 5 or so then I say 'Call me at home'" (CS1).

This interviewee described making personal sacrifices to work during lunch and after hours in an attempt to reach complainants that are often not available to engage in personal or emotional phone calls while they are at work or school. This flexibility and dedication on the part of an employee is not able to, and should not be expected to, address the larger issue that complainants are not easily supported by a helpline that is only open during regular business hours. *Therefore, CyberScan should consider offering additional hours of operation (as suggested in the subsection*).

above as well) and should make available a list of support services for both adults and youth that are more readily available. There is currently a link to Kids Help Phone (who can provide emotional support for young people) on the side of the CyberScan website, but there is no information provided on what this service is or how it relates to the services available or not available through CyberScan. There is also a link to 211 on the CyberScan website, which might be used to find support services for adults, but again no information is given explaining why this link is included. Additional supports should be explained and made easily accessible to those who are in distress/crisis and are unable to immediately reach CyberScan. In addition to linking to and explaining resources for victims looking for support outside of regular business hours, CyberScan's website should also link to resources that help bystanders learn how to best support a victim in their life. For example, MediaSmarts provides both reassuring resources for youth victims and comprehensive resources for parents/caregivers/teachers or other bystanders on the best approaches for supporting youth victims of cyberbullying or nonconsensual distribution.

Although CyberScan was designed primarily with the intention to act as a support for youth, agents report that young people very rarely contact the unit themselves. An agent in 2020 estimated that only about 1% of calls are from those under the age of 18. Another agent explained, "kids don't call us themselves, [...] it is all teachers, principals, parents or a neighbour calling, guidance councillors, it's very, very rarely a youth" (CS5). While young people may reach out to an adult in their lives that then seeks support from CyberScan, those who do not have an adult they feel comfortable reaching out to or who are not yet ready to disclose to an adult in their lives do not seem to currently be served by CyberScan. Therefore, CyberScan should consider making updates that make their support services more accessible to young people. For example, several CyberScan staff pointed out that it may be a problem that CyberScan can only be contacted by phone, as it is well known that young people are increasingly uncomfortable making initial contact through phone calls. Similar support lines internationally tend to provide multiple options for contact. For instance, Childline in the UK36 provides options for support via online chat, email, or phone and the UK's Revenge Porn Helpline<sup>37</sup> offers options for support via Facebook Messenger, email, phone, or anonymous form. Another limitation to supporting youth is that those under the age of 18 can only speak to CyberScan with the permission of their parent/guardian. This policy may be limiting in many cases. For instance, youth who have their intimate images shared without consent are often concerned about telling their parents/guardians or other adults in their lives due to fears of being blamed or shamed for having consensually shared intimate images or for having been involved in a sexual situation in which images were captured without consent (Dodge & Lockhart, 2021). In such cases, youth may be looking for information about how to tell an adult in their life or information about how to report content without telling a parent/guardian that they know will judge or punish them. In such scenarios, CyberScan's service would not be accessible to them. CyberScan would also not be accessible to youth who do not have a trusting relationship with their caregivers or to youth who know that their caregivers hold discriminatory beliefs. For example, a youth who is being bullied over social media for being gay will likely not seek help if they are required to first explain the situation to their homophobic parent/guardian to get permission. Therefore, consideration should be given to changing the policy that requires youth to get parental/guardian permission to speak with CyberScan. At the least, CyberScan's materials should be clarified to explain that permission is required and to provide alternative supports for youth who

<sup>&</sup>lt;sup>36</sup> https://www.childline.org.uk/get-support/1-2-1-counsellor-chat/

<sup>37</sup> https://revengepornhelpline.org.uk/how-can-we-help/how-to-get-in-touch/

are not willing or able to get such permission. For instance, the handout "Here to Help: CyberScan" states: "Anyone can contact CyberScan. This includes young people who feel they are being cyberbullied or are the victim of unwanted sharing of intimate images, their parents, teachers, principals, police, or other members of the public".<sup>38</sup> This handout should clarify that young people can only call with parental/guardian permission and should provide the information for alternative resources for those who do not feel comfortable disclosing to a parent/guardian.

One of the restorative approaches experts interviewed for this report asserted that there are several ways CyberScan's emotional supports could be improved by engaging restorative principles. This expert explained that, while the kind of support CyberScan currently offers is certainly *part* of what is needed to build a restorative and human-centred response to digital harm, CyberScan's response could better engage those in a victim's life as victims often experience negative consequences as a result of people in their lives acting distant or judgemental toward them in the aftermath of harm: "[Many victims of crime] will tell you that the actual fear and consequence they have following a crime is not always to do with the individual who hurt them but the ways in which they feel shunned or disintegrated [from their community]. They need to be reintegrated to their relationships with others who are afraid to ask what happened to them, or are afraid it might happen to them too, or shame them in order to keep themselves feeling like 'It couldn't be me'" (RA2). Considering these impacts on relationships, this expert suggests that CyberScan could offer options such as meeting with family members, coworkers, schools or neighbours to help them understand the harm a victim has experienced and to help them learn how to better acknowledge this harm and support the victim rather than pushing them away. They elaborated saving.

"You could see CyberScan taking advantage of [Nova Scotia's] restorative justice agencies located in communities in the province [to create] more robust capacity to engage with victims and meet their needs [...]. If you did have a victim who said, 'Not only do I want the [intimate] image down, but now everyone at my workplace, or church, or all my neighbours think these [negative things about] me' - there might be ways [to connect with those people to help them understand that] this person has been struggling and been harmed and that they might be able to help. There's a whole bunch of ways you could think about how to take a relational, restorative approach to those kinds of harms" (RA2).

This approach aligns well with research that has found that one of the most harmful aspects of nonconsensual intimate image distribution is often the feeling of shame or judgement this act can create between a victim and their close relations or community (Dodge, 2021; McGlynn et al., 2017). As Hamilton (2018) asserts, it is important to educate those in a victim's life about how best to provide support and avoid victim blaming and shaming beliefs. One of the restorative approaches experts also suggested that more robust supports could include finding ways to connect victims with others who have had similar experiences (RA2). They stress that a restorative response does not have to look like organizing restorative justice circles, rather it could look like a variety of supports and services that are geared around understanding issues relationally and looking at holistic responses that consider context, causes and circumstances (RA2).

<sup>&</sup>lt;sup>38</sup> Here to help: CyberScan unit (PDF), p.2.

Recommendation #15: CyberScan's website should link to (and provide detailed information about) support lines that are open 24/7, reassuring online resources for victims, and resources that help bystanders learn how to best support a victim in their life.

Recommendation #16: CyberScan should offer a variety of options for making contact with the unit (e.g. email, text, online chat).

Recommendation #17: CyberScan should consider allowing young people to gain support from the unit without requiring parent/guardian permission. If this is not possible, CyberScan materials should clarify that this permission is required and provide alternative support options for youth who are not willing or able to get such permission.

Recommendation #18: CyberScan should consider partnering with restorative approaches initiatives to provide broader options for healing individuals and relationships imported by digital harms.

## WARNING/EDUCATING RESPONDENTS

In approximately 2% of cases<sup>39</sup>, CyberScan staff contact respondents to ask them to remove harmful content and/or to stop further bullying. This is done through some combination of explaining the harm they are causing and describing the potential legal impacts of their actions. Although this approach can be useful, it is much less common than the responses above because complainants rarely wish to have respondents contacted. As a 2020 CyberScan agent described:

"Sometimes the complainant does not want the respondent contacted for fear that it could actually escalate the situation and make it worse... or the reasons are like 'Oh you know they are going through a hard time so I don't want you trying to contact them'. But in [a small portion] of our cases we have reached out to the respondent to kind of say 'You know this isn't acceptable, stop this behaviour' or to try to negotiate [...] with them [...and say] 'This is unacceptable, the victim may take you to court'" (CS7).

One CyberScan agent described how, in an attempt to avoid escalating the issue, some complainants use the information provided by CyberScan to contact the respondent themselves without involving CyberScan agents directly:

"I've had some cases with adults where just sending them the information on CyberScan, they felt that was helpful because then they sent it to the person that was bothering them saying 'Look if this continues, I've already contacted CyberScan and they will be in touch if... like I don't want this to continue'. And that's been enough sometimes, even to send

<sup>&</sup>lt;sup>39</sup> This is a rough estimate based on somewhat informal records kept by CyberScan staff from July 5<sup>th</sup>, 2018 to November 5<sup>th</sup>, 2020.

them the link and them to see that there is actually an organization that helps with this kind of stuff' (CS5).

In some cases, it seems that simply warning or educating the respondent that the perpetration of digital harms can have consequences is enough to end the cyberbullying or the nonconsensual distribution of intimate images. However, agents explained that it is sometimes difficult to engage adult respondents, as opposed to youth who can be engaged through the school system, because adults may simply refuse to speak with CyberScan agents: "the adult cases, they were the trickier ones for sure, because lots of them [...] didn't want to meet with us. So we might have to then draft a letter to send to them in the mail just saying who we are, explaining the legislation a bit, and asking them to stop that way" (CS4). Therefore, this response is used less frequently due to both the lack of interest in this option on the part of many complainants and the inability to compel respondents to engage with the unit. However, *in the rare cases in which this approach is used, CyberScan agents described simply speaking with respondents as often capable of resolving issues.* 

CyberScan is faced with many challenges when contacting respondents. As discussed above (See: <u>History of CyberScan</u>), some CyberScan agents working under the original *Cyber-safety Act* (2013) may have used warnings of potential legal consequences in a manner that unduly limited "legitimate *Charter*-protected speech" (Fraser, 2017). *Although continued attention will need to be paid to striking the right balance between providing warnings/education about potential legal consequences and respecting the rights and interests of respondents, the limited legal tools available under the current legislative framework makes undue limits on respondents less likely (See: Use of civil court orders). Nonetheless, it is important to consider the tone and messaging that CyberScan uses when contacting respondents. For example, CyberScan must decide how to balance warnings/education regarding potential legal repercussions with education about the harms that respondents are causing. The restorative approaches experts interviewed for this report stressed that engagement with respondents should focus on expressing that their behaviour is harming others rather than focusing on the use of law as a scare tactic. That is, potential legal consequences should be framed as a last resort rather than as <i>the* reason not to commit harm.

It is not entirely clear from the interviews how CyberScan agents balance legal warnings versus discussion of relational harms. One agent in 2016 seemed to describe focusing more on education about the harm caused than on the threat of legal actions: "[the goal of contacting the respondent was] to end [the cyberbullying] in a way that had the respondent taking responsibility for the damage they may have caused or at least an understanding or awareness of what they've done and how it impacted others" (CS3). While this agent stressed the need for respondents to understand the impact of their actions on others, the other agents interviewed in 2016 seemed to focus much more narrowly on stopping conduct through warnings about potential legal consequences. As a 2016 agent explained:

"We would seek out the respondent, the cyberbully, and the goal would be try to meet with them and explain the legislation, explain the potential consequences of the legislation, but ask if they'd agree to an informal agreement which would typically be to remove the cyberbullying content, not to engage with the victim [...] of the cyber bullying in the future, or whatever we deem appropriate for the situation we're dealing with. And if that individual agrees to those terms, then we would document everything within our database and that would be the end of the file" (CS2).

This approach demonstrates a focus on legal warnings and pressure to agree to a set of predetermined actions and limitations under threat of legal action. This response seems to disregard any meaningful discussion of relational harms or negotiation about appropriate next steps.

Although the approach taken by agents in 2020 is also somewhat unclear from interview responses, it does seem that the tone of engagement has moved more toward education and awareness of relational harms. This change in tone is likely partially due to the changing legal tools available to agents that have limited their ability to use threats of legal action. An agent in 2020 described sometimes contacting respondents without mentioning legal consequences at all: "I had a case the other day where he was just receiving a number of different unwanted messages and stuff and so I called the respondent and I said 'You know I've just received a complaint from this guy and he doesn't want you emailing him anymore', so that is kind of a little bit of a resolution by just kind of bridging that gap between both people" (CS5). However, in cases of nonconsensual intimate image distribution, which is a clearly criminalizable act, a CyberScan agent in 2020 described focusing on legal warnings as their main tactic: "Sometimes [the complainant] will say 'Could you talk to him and let him know that this could be a criminal offence even though I don't want to go that route?' So I love that it's a criminal code offence because it makes my job a lot easier, because that is the threat I can kind of use I guess... to call the respondent and say 'She is asking you to take this image down, this could be a criminal offence" (CS5). Explaining the law to a respondent and asking them to remove nonconsensually shared intimate images can act as an expedient way to stop the harm of this act; However, CyberScan agents should consider, even in these clearly criminalizable cases, how they want to balance education about the harms being caused with warnings of legal implications.

As the restorative approaches experts interviewed for this report explained, *there are several ways* to consider a more restorative approach to engaging with respondents. As one expert explained, "when they call the perpetrator [...] it is an opportunity for education and there are a variety of ways you could be inclusive, participatory, forward focused, comprehensive and holistic. All those principles could still show up [...] if they want to be restorative. But you couldn't call it restorative if they are just calling somebody and saying 'Got to take the image down, it's against the law'" (RA1). This expert further explained,

"A focus on the law [...] is what brings people together if you are taking a restorative approach, [...] but that's step two to talk about the law. Let's focus on talking about the harm that you caused rather than the law that you broke. [...] [So rather than just saying] 'Here is the law you are breaking, you should think about this', you are saying 'Hey, what's going on? Do you want to enter into a process where we figure this out?' [...] There are different questions you could ask, different things that you could say, that are meant to prompt the person to be thinking differently"<sup>40</sup> (RA1).

<sup>&</sup>lt;sup>40</sup> Ted Wachtel (2016)explains that "informal" ways of engaging restoratively (e.g. asking questions that engage relational thinking) have a "cumulative impact and creates what might be described as a restorative milieu—an environment that consistently fosters awareness, empathy and responsibility in a way that is likely to prove far more effective in achieving social discipline than our current reliance on punishment and sanctions".

In working toward taking a more restorative approach, agents should also consider what supports respondents might need to deal with the issues or circumstances that led to their perpetration. Taking a relational approach, supports should be human-centred and not just victim-centred so as to recognize and address "the experiences, needs, and perspectives" of all the parties involved (Llewellyn et al., 2014). CyberScan should consider the ways perpetrators of harm could be better supported to acknowledge the harm they have caused, to change their behaviour, to help heal harm caused, and/or to receive support for their own needs. Addressing the needs of all parties is especially important in the context of bullying and cyberbullying as the literature finds that perpetrators of bullying are often victims of bullying as well (Beran et al., 2015). As the director of education for MediaSmarts explains, "it's not at all uncommon, for example, for someone to be the aggressor in one relationship and the target in another, or for victims to try to retaliate against their harassers. [...] In classroom bullying, for instance, high-status youth often keep their bullying 'under the radar' until the target retaliates - at which point she is usually the one punished. In a painful irony, cyber-bullies often use mechanisms designed to fight bullying as a tool for bullying by threatening to 'report' their targets".<sup>41</sup> Therefore, the "victim" and "perpetrator" roles may not always be so clear or consistent. As one CyberScan agent described, it can also be the case that a bully begins to be bullied for their actions in a way that creates more harm rather than creating accountability: "Public shaming is a big thing on the internet, all of a sudden the whole small town is talking about this kid that did this [bullying], and its adults actually publicly shaming this youth" (CS5). This agent explains that, in youth cases especially, the family of the respondent is also sometimes cyberbullied for being "bad parents" in the aftermath of harm (CS5). These examples demonstrate that a simple victim/perpetrator dichotomy does not always exist in cases of cyberbullying<sup>42</sup> and that addressing the particular issues in a case will often require attention to the needs of all parties and impacted relationships (Cyberbullying Hurts: Respect for Rights in the Digital Age, 2012; Fairbairn et al., 2013). It is also necessary for CyberScan to learn from the actions of individual respondents to determine what broader educational and systems-level changes are needed to prevent or better address future acts of harm (e.g. a lack of knowledge about the harms of nonconsensual intimate image distribution in a particular age group or community could signal the need for further public education about this act that is targeted at that particular group).

> Recommendation #19: Approaches to engaging respondents should be consistently assessed to ensure they are not unduly limiting respondents' legitimate expression.

> Recommendation #20: CyberScan agents should consider taking a more restorative approach to engaging with respondents and should carefully assess how they are balancing discussions of relational harms with information about potential legal consequences.

<sup>&</sup>lt;sup>41</sup> https://mediasmarts.ca/blog/shades-grey-rethinking-cyberbullying-interventions

<sup>&</sup>lt;sup>42</sup> The victim/perpetrator roles can also be more complicated in cases of nonconsensual intimate image distribution in which images are shared without consent because the person "had received those images against their will, making them both victims and perpetrators" (Naezer & Oosterhout, 2021, p. 9).

Recommendation #21: CyberScon should consider the ways perpetrators af harm could be better supported to acknowledge the harm they have caused, to change their behaviour, to help heal harm caused, and/or to receive support for their own needs.

## RESPONSES TO YOUTH CASES

This section discusses the specific responses that CyberScan provides in youth cases. The first subsection discusses CyberScan's school-based responses to individual youth complainants and respondents involved in cases of cyberbullying or nonconsensual intimate image distribution. The second subsection discusses the educational presentations for youth that CyberScan often provides as a preventative measure and/or in the aftermath of an act of cyberbullying or nonconsensual distribution. The third subsection discusses CyberScan's approach to education on the topic of nonconsensual intimate image distribution. The final subsection discusses specific concerns that arise in responding to youth (under the age of 18) cases of consensual and nonconsensual intimate image distribution due to the problematic labelling of these acts as "child pornography".

## SCHOOL-BASED RESPONSES TO YOUTH COMPLAINANTS & RESPONDENTS

Prior to 2016, CyberScan agents regularly worked closely with school principals to respond to individual cases of digital harm among youth by meeting with the various parties involved. However, agents interviewed in 2020 explained that they are now most often contacted by school principals after a case has already been dealt with by the school, and the principal simply requests that CyberScan provide a "cyber safety" presentation. Agents in 2020 were unsure why exactly CyberScan has largely moved away from the more involved school-based responses described in 2016: "We could [meet with the parties involved], but we don't do it a whole lot, surprisingly. I've done it a few times in the schools, where actually the teacher and myself and the two parents and both youth all sit down and kind of talk about what happened and how we are going to move forward and that kind of thing, but typically we don't do a whole lot of that" (CS5). It seems that one reason for this change in approach is that schools currently view CyberScan largely as a resource for educational presentations in the aftermath of cases: "Typically if the school calls and there is an issue between two students [...] the school may have already dealt with it through a suspension or something, but then like they are saying 'Can you come to the class and speak to the whole class about some of the detrimental effects of cyberbullying or of passing an intimate image without consent?" (CS5). Because it is unclear why exactly the relationship between CyberScan and school has changed, CyberScan and schools should work together to explore whether the current relationship uses CyberScan to its full potential or whether other supports and responses could be offered.

As this subsection analyzes CyberScan's school-based responses to individual youth complainants and respondents, it draws primarily from interviews with agents who worked more closely with schools prior to 2016. Agents interviewed in 2016 reported that their assistance with school-based responses usually involved the following steps: CyberScan is contacted by a school official (usually the school principal) regarding a case of cyberbullying or nonconsensual intimate image distribution; CyberScan speaks with the complainant and their caregiver(s) to gather evidence about the incident; along with the principal, and potentially other parties (e.g. school councillor), CyberScan meets with the complainant and their caregiver(s) to provide education regarding cyber safety; along with the principal, and potentially other parties (e.g. school resource officer), CyberScan meets with the respondent and their caregiver(s) to have them remove any remaining harmful digital content, create an informal agreement to stop the behaviour, and provide them with education about the relevant civil and/or criminal laws that could apply if they continue this behaviour (CS1). Prior to 2016, CyberScan agents were regularly traveling to schools throughout the province to hold these hour-long school-based meetings with complainants and respondents (CS2). Agents in 2016 described this approach as quick and effective: "You can have back-to-back meetings and resolve the issue as quickly as possible within a day or two" (CS2). While expediency is helpful in terms of the initial response, immediate interventions should be followed by deeper and ongoing responses that address the core issues revealed by a case. Both restorative approaches experts stressed that responses to youth cases should not simply be aimed at getting an agreement from the respondent that the harmful behaviour will stop, but rather should aim to understand and address the "contexts, causes, and circumstances" behind the harmful act and to "build a more robust approach to safety and wellbeing in schools" (RA2). As CyberScan agents drop into a school for a few hours or days and then leave, they should work with schools and caregivers to cocreate plans for providing ongoing and holistic responses after they have left.

From a restorative perspective, responses to individual cases of harm should act as a catalyst to consider what relational and systems-level changes are needed to address the broader issues that are revealed by individual cases. Despite being envisioned early on as a resource for providing a robust restorative approach in schools, CyberScan does not currently work with schools to consider ongoing interventions in the aftermath of harm (See: Taking a restorative approach?), Rather, CyberScan's standard intervention currently entails providing a short "cyber safety" presentation, the limits of which are discussed in more detail in the subsection below. One of the restorative approaches experts explained that the early vision for CyberScan was that agents would help schools respond to individual cases to immediately stop the harmful behaviour, but would then take the time to say "Now let's talk about what's going on here more broadly" (RA1). For example, an individual case of homophobic cyberbullying would be a catalyst to ask: What about the school and community environment is sending the message that homophobia is acceptable? And what changes would need to occur at the level of interpersonal relationships, school policy/practice, and community to address this? Helping to coordinate a robust approach, a CyberScan agent might work in collaboration with school staff, community organizations, and students to craft a plan that, in the example of homophobic bullying, might include supporting the creation of a gay-straight alliance with the help of the Youth Project, adding discussions of LGBTQ+ rights and historic figures into various class curriculums, educating teachers and school staff on how to ensure they are modelling the use of inclusive language and are addressing instances of homophobic bullying in the classroom, and ensuring that school policies and practices support equality and inclusion. An individual case reveals that "a person has a particular view of what's okay or lacks the understanding of how this could impact a person", and that information can be used to "inform what the guidance counsellor is talking to kids about, what kinds of conversations teachers are having day-to-day in a classroom, and it ought to inform a whole bunch of other things that we do in terms of the school system" (RA1). One of the restorative approaches experts explained that CyberScan should look at broader "systems, policy, practice, or messaging that needs to change"

within a school because, "if they aren't feeding [what they are learning from individual cases] back up to the system and doing things different in the system, then what we have are [...] responses that make things marginally better for [individual students] but then we just have a new crop of students come in the next year and the whole cycle starts again" (RA1).

In terms of ensuring ongoing impacts from CyberScan's interventions in youth cases, it is also necessary for CyberScan agents to reflect on how they balance legal warnings versus helping the respondent understand the harms and relational impacts of their actions. As discussed above (See: Warning / educating respondents), it is important to help all wrongdoers, but especially youth, to realize the relational impacts of their actions on others rather than primarily using scare tactics about how potential legal consequences could negatively impact them. As a restorative approaches expert explained, legal warnings have "a short term impact and, in the school system especially, we should be very worried about the long term implications and having people understand the impacts of this behaviour in a way that isn't just talking about the legality" (RA1). A 2016 agent described CyberScan's approach to meeting with youth respondents in the following way: "The first thing we would do is explain the Cyber Safety Act, [...] we'd go through the law and what the law means, we'd explain that we'd like to resolve everything informally in the first instance, but we'd explain what the legal consequences were if it continues. And then if it [...] involved intimate images, we'd explain what the criminal law is as well and go through all that with them" (CS2). This very law-focused approach, which was described by several agents in 2016, is not the most impactful way to engage youth respondents. Youth are unlikely to refrain from harmful behaviour just because there is a law; Rather, they are more likely to change their behaviour if those close to them express their disappointment in the behaviour and help them understand the relational harms their behaviour is causing (Cyberbullying Hurts, 2012, p. 314; (Morrison, 2002, p. 6; Russell & Crocker, 2016). As restorative approaches experts assert, responses to youth wrongdoing should help youth understand how their actions negatively impacted "relationships in the school and wider school community", rather than simply asserting that it is wrong because it violated the law or school rules (Morrison, 2002, p. 6; Russell & Crocker, 2016). As Wendy Craig reported to the Senate of Canada, bullying is a relationship problem that requires relationship solutions (Cyberbullying Hurts, 2012). Therefore, youth respondents should be helped to understand the consequences of their behaviour in a way that develops "relational thinking" (Morrison, 2002, p. 6; Russell & Crocker, 2016) and treats legal education as a carefully communicated secondary goal.

CyberScan should also carefully consider which people are most appropriate to bring into meetings with youth respondents. *Namely, bringing a school resource officer into these meetings, which agents in 2016 described as a regular occurrence, could move the meeting toward a less successful "scare tactic" or "law and order" approach.* As one of the restorative approaches experts commented,

"[I] worry about automatically bringing [...] the school resource officer in. [What I would say to principals] is 'Stop bringing your resource officer in to scare those kids straight'. If you want to bring those resource officers in it could be to say 'Hey, [...] this is why I'm worried about you' or 'This is the sort of ripple effects that you are having on the families and the community', to help a young person understand what you see as a police officer as the impact of their behaviour. But not focusing in on [...] 'Right now I could arrest you!

Right now you're getting a caution, but do it again and I'm going to arrest you!' [...] [When deciding whether to bring] that resource officer in, [don't do it] unless they are bringing them in to talk to that child in a way that will help them expand their understanding of the impact, otherwise you are just doing a law and order approach" (RA1).

The inclusion of school resource officers should also be questioned due to growing uncertainty regarding the appropriateness of using police as a resource in schools, especially considering evidence that their presence has particularly negative impacts on marginalized youth (Boyd, 2020; Vitale, 2017). As CyberScan agents are able to respond informally in almost all instances of digital harm, a representative of the criminal justice system may be an unnecessary presence in these meetings, especially as one of CyberScan's core roles is to provide any legal insight that may be needed. Instead of including police officers, attention could be given to who could be helpful in addressing the specific case at hand. For example, in a case involving nonconsensual intimate image distribution it could be useful to have a sex educator present who can speak to the importance of sexual consent.

Finally, CyberScan should also carefully consider the messages they communicate to complainants in their school-based responses. CyberScan agents in 2016 described providing youth complainants with "cyber safety tips" in the aftermath of harm. These tips included telling complainants to use privacy settings to limit who can see their social media profiles and to limit their social media contacts to include only those they know in real life (CS4). In most cases reported to CyberScan, the perpetrator of harm is someone known to the complainant and, therefore, such "cyber safety" precautions taken by the complainant would not have prevented the harm and may not feel like relevant support in the aftermath of bullying involving their peers, expartners, or others that they interact with in their integrated online/offline lives. Some approaches to providing "cyber safety" tips could also make the complainant feel as if they are being judged for the harm they experienced. An agent in 2016 described that agents would sometimes review a youth complainant's social media profile and provide "cyber safety" advice based on what they saw: "We would discuss stuff that wasn't specific to the investigation but that I was able to view online as I was investigating, you know posting provocative photographs that are open to the public that anyone can take and post anywhere else, and just give them some safety tips about that" (CS4). Complainants might find it an invasive or shaming experience to have their personal social media accounts examined and critiqued by a government enforcement agent in this way. While it can be useful to help youth think critically about some of the things they might want to consider when crafting their online presence, agents should avoid making moral judgements or giving prescriptive advice about a young person's self-expression. In cases involving digital forms of sexual violence, "eyber safety" tips could especially come across as blaming or shaming. For instance, in the aftermath of nonconsensual intimate image distribution, it can be harmful to provide responses that assert the victim is responsible if they consensually shared intimate images that were later shared without their consent (See: Education regarding nonconsensual intimate image distribution). Therefore, CyberScan agents must research best practices in terms of education and support for complainants to ensure their messaging is appropriate, relevant, and avoids victim blaming or shaming. Useful resources for providing appropriate supports include, for instance, Project Shift's guide for supporting girls who are impacted by digital harm<sup>43</sup>. This guide includes practical tips for supporting girls, such as ensuring that responses to digital harm do not make

<sup>43</sup> https://mediasmarts.ca/sites/mediasmarts/files/guides/ywca-guide-for-trusted-adults.pdf

"girls feel scared and helpless [...] by exaggerating the risks of being online [...] and instead make sure they feel that they have the tools to deal with whatever negative experiences they face and that they have trusted adults they can count on if things go wrong"<sup>44</sup>.

Recommendation #22: CyberScan and schools should work together to explore the most meaningful and useful ways they could collaborate moving forward.

Recommendation #23: CyberScan should consider taking a more restorative appraach to youth cases that provides halistic/angoing responses, carefully considers what parties are most appropriate to including in discussions with youth, focuses on the relational impacts of wrongdoing, and uses individual cases of harm as a catalyst to consider what policy, relational, and systemslevel changes are needed to address the deeper issues revealed by a case.

Recommendation #24: CyberScan agents must research best practices for supporting and educating youth impacted by cyberbullying or nonconsensual intimate image distribution to ensure their messaging is appropriate, relevant, and avoids victim blaming or shaming.

## EDUCATIONAL PRESENTATIONS

*CyberScan's mandate includes providing educational presentations on cyberbullying and nonconsensual intimate image distribution to Nova Scotians. This mandate has primarily been responded to in the form of "cyber safety" presentations for youth.<sup>45</sup> A significant amount of CyberScan agents' time is spent providing these presentations. As an agent in 2020 explained, "there is only two of us doing this right now, it works out to about 20 presentations a month [...] so it's still a big part of our job, and we get lots of requests from schools [...] to do them" (CS5). Between 2013 and 2017 agents provided over 900 cyber safety presentations<sup>46</sup> and between July 5<sup>th</sup>, 2018 and July 5<sup>th</sup>, 2020 agents provided 464 presentations (See infographic below). A 2016 agent explained that these presentations are aimed primarily at meeting CyberScan's prevention goals by educating "the province about the law and educating Nova Scotians about the harm of cyberbullying and that it's illegal to do it" (CS2). It is necessary to closely analyze whether the educational approach taken in these presentations is appropriate to the goal of preventing cyberbullying and nonconsensual intimate image distribution.* 

<sup>44</sup> https://mediasmarts.ca/sites/mediasmarts/files/guides/ywca-guide-for-trusted-adults.pdf, p.23-24.

<sup>&</sup>lt;sup>45</sup> Although CyberScan also provides some presentations to adults (generally government staff or community service providers) on the *mandate* of the CyberScan unit, this subsection focuses specifically on the cyber safety presentations provided to youth. This focus is taken both because presentations for youth are more common and because suggestions for improved communications about CyberScan's mandate are already provided in the section above titled <u>Communicating CyberScan's role</u>.

<sup>&</sup>lt;sup>46</sup> Nova Scotia, Legislative Assembly, Hansard, 63<sup>rd</sup> Leg, 1<sup>st</sup> Sess, No 27 (12 October 2017) at 1166.

CyberScan's cyber safety presentations for youth are typically provided in schools and are delivered either to individual classes or in a school assembly. Presentations are often requested with the general goal of prevention: "we'll just get a call where a principal says, 'We have all new grade 6 students starting this year, do you mind meeting with all the grade 6 students just to get them off on a good foot and talk about cyber safety?" (CS5). At other times, presentations are requested in the aftermath of a particular act of digital harm or to try to address ongoing acts of harm (CS2). Agents generally expressed feeling that these cyber safety presentations are effective. They provided examples of positive impacts such as the takedown of an anonymous rumour account following a presentation in a high school assembly (CS2) and an elementary school student reporting an incident of cyberbullying because they learned through a presentation that it was against the law (CS5). Between July 5th, 2018 and July 5th, 2020, agents also measured success through having youth complete surveys following CyberScan presentations. The image below is a portion of an infographic made by CyberScan to display the results of these surveys. As shown in this infographic, the majority of youth surveyed by CyberScan reported that they learned tips to improve their online safety. While the results of this survey imply that CyberScan's educational approach is successful, it is necessary to assess whether the learning outcomes being measured are appropriate for preventing cyberbullying and nonconsensual intimate image distribution.

# PRESENTATIONS

464

12,893

Total number of presentations given on cyber-safety and the mandate of the CyberSCAN unit.

Total number of youth and adult participants who took part in the presentations.

	YOUTH SURVEYS			
2	Did the presentation make you think about doing more to protect your personal information when online?	84% Yes	16% No	n = 1.027
?	Do you agree with the statement: "The presentation taught me at least one new tip to improve my safety when online?"	<b>93%</b> Agree	7% Disagree	n = 1.023
?	In the future, how likely are you to use at least one of the online safety tips from the presentation?	93% Likely	7% Not Likely	n = 1.025

Based on the survey questions asked (See infographic), as well as interviews with CyberScan agents and a review of the PowerPoint slides used for their cyber safety presentations, *it seems that CyberScan's presentations are aimed primarily at giving youth "cyber safety" tips (e.g. limit who can see your social media profile, don't accept friend requests from strangers, don't share your home address online) that are more appropriate for avoiding instances of harassment, luring, or stalking by strangers than for preventing cyberbullying or nonconsensual intimate image distribution. While these are generally desirable tips for youth living in the digital age, there are* 

several reasons why they do not necessarily align with the goal of preventing or responding to cyberbullying and nonconsensual intimate image distribution. For example, the vast majority of CyberScan's cases involve a respondent and complainant that are known to each other offline, yet CyberScan's cyber safety tips seem to focus largely on addressing "stranger danger" scenarios and online privacy infringements. A CyberScan agent in 2016 explained that their cyber safety presentations teach youth:

"About privacy settings, [...] about how easy it would be for a stranger to find out where you live with your GPS on. [...] So just trying to build awareness that when you're on social media and you're in the comfort of your own home, and you have like your GPS on, everyone in the world physically can see where you are. And that was the other big topic was about not talking to strangers online. Teaching youth [...] how to put your privacy settings on. How to keep yourself safe." (CS4)

A 2020 agent similarly described their presentations as helping youth to "realize how open their profiles are" and to ensure that only people they know offline can see their social media profiles: "[We tell youth to] make sure you are aware of who can see your posts and who can contact you. Accept only messages from those on your friends list and make sure only friends can see your location. Tidy up your friends list and delete those you don't actually know" (CS5). The PowerPoint presentation for youth in 2020 likewise provides safety tips that are primarily aimed at avoiding harm/privacy-infringements at the hands of strangers, such as: "Don't post personal information online (no phone number, address or school); Use only your first name or nickname; Use privacy settings; Make sure your device has a lock code"<sup>47</sup>.

There is a clear disconnect between these cyber safety tips, which are focused on avoiding the exposure of personal information and location to strangers<sup>48</sup>, and the kinds of cases CyberScan most often responds to (i.e. cases in which complainants and respondents are known to each other offline and bullying/harassment is often occurring both online and off <sup>49</sup>). As Fairbairn et al.'s (2013) study of digital sexual violence found, "because the majority of sexual violence associated with social media is perpetrated by someone known to the individual, blocking programs and privacy controls are less likely to be effective prevention mechanisms" and preventative education "should recognize that online victimization is not primarily 'stranger-danger'" (p. 6). They recommend that online safety advice should be treated as a "tip for protection, not a road to prevention" (Fairbairn et al., 2013, p. 6). Likewise, best practices in youth education for cyberbullying more generally tend to avoid the kind of cyber safety model that CyberScan currently utilizes. As the education director for MediaSmarts explains, interventions that focus on a cyber safety model, rather than addressing complicated relational dynamics and discriminatory beliefs, "are bound to fail"<sup>50</sup>. One of the restorative approaches experts likewise commented on the inappropriateness of the cyber safety model for addressing these relational issues saying:

<sup>&</sup>lt;sup>47</sup> CyberScan PowerPoint slides for grades 4,5, & 6.

<sup>&</sup>lt;sup>48</sup> At times, it even seems that a "cyber safety" focus has resulted in CyberScan's presentations veering into discussions of adult predators luring children online, which is a very different issue than those peer-to-peer cases that CyberScan was created to respond to. As an agent in 2016 described, "we talk about child luring cases, child protection, and child exploitation cases" (CS4).

<sup>&</sup>lt;sup>49</sup> As a CyberScan agent described, "I mean cyberbullying usually doesn't stop at cyberbullying, so there's also going to be some bullying going on at school too, you know" (CS2).

<sup>&</sup>lt;sup>50</sup> https://mediasmarts.ca/blog/shades-grey-rethinking-cyberbullying-interventions

"[Acts of cyberbullying and nonconsensual distribution] are almost always tied up in complex emotional reactions, responses, and pressures around sexuality, identity, relationships, and hurt. So it's just tone deaf to turn up and think that privacy or technology is the problem, it just gets the problem wrong. And then [youth] really don't listen to you if you don't have the problem right" (RA2). *The cyber safety model is also problematic because it puts the onus squarely on potential victims to avoid being harmed and does little to address why youth harm each other and what would need to change about their behaviours, and the contexts and circumstances around them. to make this less likely.* Research has found that when "children and youth are primarily educated about digital technologies through an 'online safety model' that focuses on protecting themselves and avoiding 'risky' activities", they may learn to responsibilize victims for the harms they experience rather than learning what ethical behaviour looks like (Mishna et al., 2020, p. 419; Naezer & Oosterhout, 2021). Education that focuses primarily on discussions of the victim's role in avoiding harm can be counterproductive by invisibilizing the actions of perpetrators and implying that the cultures that support bullying are natural and unchangeable (Mishna et al., 2020).

The current cyber safety approach does not seem to address the kinds of harmful interpersonal conflict, discriminatory bullying, or digital sexual violence that CyberScan was created to respond to. Demonstrating the incongruence between "cyber safety" tips and the core issues CyberScan was created to address, the harm committed in the Rehtaeh Parsons case<sup>51</sup> (i.e. the catalyst for creating the CyberScan unit) would likely not have been prevented or lessened by the current approach to cyber safety education. Nothing Rehtaeh could have done in terms of securing her privacy settings or avoiding strangers online would have addressed the sexist bullying and victim blaming/shaming that she experienced from her peers online and off. To alleviate the harms in cases such as this, education would need to address sexist and victim blaming/shaming beliefs and teach students how to support victims of sexual violence and nonconsensual intimate image distribution. As Rehtaeh's father put it in a recent interview, "a lot of people think that Rehtaeh died because she was cyberbullied — and it played a part of that — but a bigger part of her entire story really is a story about victim-blaming and misogyny" (Cooke, 2021). Likewise, Segal's review of the handling of the Rehtaeh Parsons' case states, "I wholeheartedly agree that the true solution to the problem lies in the evolution of societal norms related to sexual assault specifically, and gender equality more broadly" (Segal, 121). CyberScan's current cyber safety model of education does not seem to be aimed at challenging the culture beliefs that fuel the harms of sexist bullying, victim blaming/shaming, or other discriminatory beliefs that are often present in the most harmful experiences of cyberbullving and nonconsensual intimate image distribution. When asked whether CyberScan's presentations address discriminatory beliefs (e.g. sexism, victim blaming/shaming) or discuss healthy relationships, an agent in 2020 responded:

"No, we don't. That would be great, and I know the schools would like something like that, but we only have like 40 minutes. We basically talk about the social and legal detrimental effects of cyberbullying and passing an intimate image, and some of the things that could result from that, and then we always talk a lot about cyber safety. But we don't [talk about healthy relationships or discrimination]. And we're not really educators either, so our [...]

<sup>&</sup>lt;sup>51</sup> Parsons died by suicide in the aftermath of having an intimate image of her (captured during an alleged sexual assault) nonconsensually distributed and used as fodder for sexist and victim blaming/shaming bullying and harassment by her peers.

presentation is very specific [to cyber safety] [...]. But yeah [it would be good to] even be teaching them what is a healthy relationship, or that if someone is continually asking you to do something you're uncomfortable with, like that is really not okay. And I don't know if [the schools] teach really anything like that even" (CS5).

As agents do not currently address the core issues that underly cyberbullying and nonconsensual intimate image distribution, and do not have training in education, much work is needed to make CyberScan the robust educational resource that it could be.

While CyberScan's current educational approach seems to primarily responsibilize potential targets to avoid harm through cyber safety tips, best practices in addressing cyberbullying and nonconsensual distribution (such as those described by MediaSmart<sup>52</sup> and by education scholars<sup>53</sup>) assert that education should be focused on challenging discriminatory beliefs, unequal power dynamics, and exclusion of those who are different. Education should aim to create "a culture where bullying is not seen as the norm "54 and should teach youth the importance of healthy/ethical relationships, consent, diversity/inclusion, and empathy. CyberScan agents should consider working in collaboration with organizations in the province that specialize in providing education to youth on these topics. For instance, the educator for the Youth Project specializes in providing workshops on diversity/inclusion and would be well-suited to help address issues of homophobic or transphobic bullying in schools. In regard to consent and healthy relationship education, CyberScan might seek support from regional Sexual Health Centres that can provide multiweek programming that embeds conversations about nonconsensual intimate image distribution and digital relationship abuse into broader discussions of healthy relationships and consent. Adequate resourcing to community and government organizations that provide education on these topics is needed to provide robust educational responses to the core issues that underly digital harms.

Education will also be more successful if it speaks to the particular issues a school is dealing with, is cocreated by those in the school or community, and engages youth rather than "talking at" them. One of the restorative approaches experts suggested that, when a school requests a cyber safety presentation from CyberScan, agents could begin by discussing what particular issues the school is facing and offering more engaging and tailored options than a standard presentation:

"Say to the school 'Look tell us what you're hearing, what are the trends here, tell us a little bit about what kids think', and then go back and look at the resources that [CyberScan] has available and [...] come back to the school and say 'Here's how we could help.' [...] So come back to that school with some material that is relevant to the kids, maybe we've designed some talks with the kids, we have some focus groups planned for the kids, like we could do a whole project right? [...] [CyberScan could say] 'Well we don't just do presentations... I could just give you the slide deck and your guidance councillor could do this presentation if that's all you want. You don't need the CyberScan investigators to come

<sup>52</sup> https://mediasmarts.ca/blog/shades-grey-rethinking-cyberbullying-interventions

<sup>53</sup> https://www.mcgill.ca/definetheline/resources/resources-educators

<sup>&</sup>lt;sup>54</sup> MediaSmarts explains that making "not bullying" the norm can be done, in part, through a process called "social norming" in which "positive behaviours are reinforced by making members of a group aware of how common they are" and how much less common harmful behaviours are than youth assume (See: <u>https://mediasmarts.ca/blog/shades-grey-rethinking-cyberbullying-interventions</u>).

in [...] for that. We could do so much more. [...] We could go in and we could facilitate conversations, or we could meet with families, or we could come in and work differently, work restoratively, with you" (RA1).

Education will be more successful if it is tailored to a particular student context and is provided through interactive workshops/discussions rather than through a standard presentation. Rather than providing cyber safety tips that could be passed on through a video presentation without bringing in CyberScan, class time could be spent engaging with students about their beliefs regarding the challenges that digital technology can bring to having respectful relationships, the supports they use when they are struggling, and the ways that they want the school to help support them: "[Young people] are way more experts on what actually leads to escalating tensions online and what would help keep them safe or get help than any of those people standing in front of the classroom are" (RA2). There is a great deal of evidence that providing presentations that "talk at" young people, rather than engaging them in open discussion or change making activities, will have limited impacts and may be simply tuned out by youth<sup>55</sup>. As a restorative approaches expert put it, "if you're going to spend curricular time, don't just have them come and do a little presentation, [...] no one learns that way" (RA2). Rather education can help "build the capacity for people to understand their obligations to one another and impact on one another", "to gain the capacity to talk about difficult things", and to begin thinking critically about the ways they interact online (RA2). Project Shift is an example of an educational resource that provides questions to start this kind of open conversation with youth about the challenges and supports they need to deal with harms and relationships in a digital world. This resource suggests asking questions such as: "What questions do you ask yourself before you post or share something?" and "What would you do if you saw someone being harassed online?" 56.

By cocreating educational responses with school staff or community organizations. CyberScan would also be able to ensure that educational interventions build capacity for ongoing responses once CyberScan agents leave. One of the restorative approaches experts asserted that it is not the most impactful approach to have a CyberScan agent, who students have no pre-existing or ongoing relationship with, provide a single presentation to students (RA1):

"Kids will tell you that [...] having an expert come in that the kids don't know and don't have a relationship with does not have the same impact as the people they have a relationship with, so the teachers they trust, the guidance councillors they trust. So it's not that somebody can't come in and technically do a good presentation and share information... but that information lands differently for the children than if that very same information was part of a regular conversation that a teacher or other staff member is having with the kids every day [...]. A restorative approach to cyberbullying [...] cannot be only on the plate of the CyberScan unit, there has to be this relationship with the school system that says, 'Here is this unit, how can we leverage this relationship and this very good resource to work differently with schools to address cyberbullying?" (RA1)

Education experts and restorative approaches experts warn against "one-time interventions", as it is much more effective and engaging to provide "programs that are planned to go on through the

<sup>55</sup> https://mediasmarts.ca/blog/shades-grey-rethinking-cyberbullying-interventions

<sup>&</sup>lt;sup>56</sup> https://mediasmarts.ca/sites/mediasmarts/files/guides/ywca-guide-for-trusted-adults.pdf, p.25.

entire school year" that help create a day-to-day environment of care and trust in which young people are able to ask for support, have difficult conversations, and learn ethical behaviour (Cyberbullying Hurts, 2012, p. 82; RA1; RA2). Instead of providing a single 40-minute presentation, CyberScan could, for example, help design a series of workshops on healthy relationships on and offline to be provided by the school's guidance councillor throughout the year. Using this approach, students learn about these issues in an ongoing way and receive these messages from those in their lives that they can go to for support. Likewise, cocreating education with community organizations allows young people to be familiarized with and seek supports from those who will continue to be present in their community or school. While a CyberScan agent might present on the topic of nonconsensual intimate image distribution in Amherst and then drive back to Halifax, a similar workshop could be delivered by Cumberland County's Sexual Health Centre as part of their multi-week healthy relationship education and could end by encouraging youth in Amherst to stop by the centre if they ever need additional information or support on this topic. When educational approaches are cocreated with school staff or community organizations they can: be tailored to the specific school environment; include ongoing workshops, focus groups, or class projects; help encourage access to follow-up supports; and help support a positive school and community culture that is actively engaged in developing healthy relationships.

As discussed above in terms of responses to individual cases, educational approaches will also be more impactful if they focus on relational harm rather than legal consequences. A 2016 agent described providing educational presentations that are quite focused on legal warnings: "[we educate] the young people about [...] cyberbullying and the law, [...] about online safety and [making them] aware there is a law" (CS2). Agents in 2020 described presentations that were somewhat more balanced between discussing harm and providing legal education, however educational approaches may still lean too heavily on legal scare tactics by sometimes including police officers as co-presenters and focusing more on legal warnings than relational impacts (CS5). As one of the restorative justice experts explained, presentations focused on legal warnings may have immediate impacts by scaring youth into compliance, but are less likely to effect long term behavioural change (RA1). Impactful education must go beyond making youth "afraid of punishment", and should rather help youth put themselves "in another person's shoes". 57 An overemphasis on the law could also backfire in several ways; For instance, youth victims of cyberbullying or nonconsensual distribution may be less likely to seek support if they believe it will necessarily become a "big deal" by starting a legal process or leading to the criminalization of their peers (Choo, 2015; Dodge & Lockhart, 2021).

Both the cyber safety model and a focus on legal impacts can sometimes leave young people feeling fearful and unempowered. However, education experts assert that educational interventions should instead help young people feel empowered to make positive change, to find supports when they are in need, and to support others (Johnson, 2016). As Nik Basset, Education and GSA Coordinator for the Youth Project states, young people should leave an educational workshop feeling empowered to make their school and community better (e.g. to start a GSA or student club that addresses oppressive cultures in their school and community) and more equipped to support themselves or a peer that is struggling (e.g. knowledge of supports and ideas about how to search for additional resources), rather than leaving feeling hopeless or scared<sup>58</sup>. For example, a workshop

<sup>57</sup> https://mediasmarts.ca/sites/default/files/lesson-plans/lesson promoting ethical behaviour online 0.pdf

<sup>58</sup> Personal communication, March 2021.

about gender identity could end with questions such as: How would you support a friend that is being bullied for being trans? What could you say to help them feel better? Where might you find helpful resources for them online or in the community? *In a well-intentioned attempt to protect young people, "cyber safety" presentations often describe horror stories of digital harm to try to scare youth away from risky behaviour, but it is necessary to recognize that youth will encounter challenges, make mistakes, and take risks and they, therefore, also need to be supported to imagine what it looks like when someone who is harmed is well-supported and to consider what their role could be in providing positive supports. Education should help young people normalize supportive behaviour<sup>59</sup> and help them understand that they "have the ability to make practical contributions in responding to incidents of cyberbullying, such as by taking steps to denounce bullying rather than being a complicit bystander, or to help bullying victims after the fact by reassuring them that the treatment they received from the bully was inappropriate" (<i>Cyberbullying Hurts*, 2012, p. 58). Youth should also be informed that, while harm can occur online, the online world has also allowed young people access to a multitude of supports and resources and is often a place for, especially marginalized, youth to find supportive communities (Mishna et al., 2018).

Recommendation #25: CyberScan should move away from the "cyber safety" model of education and should instead seek to addresses the care discriminatory and relational issues that underly cyberbullying and nanconsensual distribution. Addressing these care issues will require angoing and interactive education on healthy/ethical relationships, diversity /inclusion, consent, and empathy.

Recommendation #26: The province should ensure adequate resourcing of government and community organizations that can help support the need for engaging and impactful education to prevent digital harms.

Recommendation #27: To ensure education is relevant to particular school contexts and allows youth to access continued support in their communities, educational approaches should be cocreated with school staff or community organizations that young people are familiar with and can easily access for ongoing support.

Recommendation #28: Educational approaches should avoid an overreliance on legal warnings and scare tactics, and instead help youth feel empowered to make change, seek support, and support others.

#### EDUCATION REGARDING NONCONSENSUAL INTIMATE IMAGE DISTRIBUTION

CyberScan's educational approach to the issue of nonconsensual intimate image distribution requires individual focus. Because nonconsensual distribution is a form of sexual violence, it is particularly important for education on this topic to be informed by best practices and to avoid

<sup>59</sup> https://mediasmarts.ca/digital-media-literacy/digital-issues/online-ethics

victim blaming/shaming narratives (Fairbairn et al., 2013). When asked about their approach to education on nonconsensual intimate image distribution. CyberScan agents primarily described education aimed at changing the behaviours of those who consensually share images (i.e. targeting the behaviours of potential victims rather than potential perpetrators of harm). As an agent in 2016 stated:

"We explain about potential consequences of sexting in the future, [...] how these photos can pop up five, ten years down the road too, you know. We talk about how once you take that intimate image of yourself on an electronic device and you hit that send, you don't have control of that photo anymore. We use an example, that sexting is like going to Costco or Walmart and asking them to print 1000 photos of you naked and walking around handing these photos out to people. We ask 'Would you do that?' and they of course all go 'No', but if you hit that send button one time thousands of people can end up having copies of it" (CS2).

By asserting that trusting someone with your nude image is the equivalent of purposefully handing out one's nude image to strangers, this example ignores the actions of perpetrators of nonconsensual distribution (who violate a person's trust, privacy, and bodily autonomy through their actions) and instead focuses the blame on the consensual act of the victim (and frames the victim's act as stupid/naive and worthy of shaming). Scholars have found that education campaigns directed at the potential victim's behaviour can act to affirm the harmful belief that victims of this act are "bad, dirty, stupid and/or dangerous" (Albury et al., 2017; Angelides, 2013; Naezer & Oosterhout, 2021, p. 7). That is, education that focuses primarily on the consensual image creator can reinforce rather than challenge harmful victim blaming/shaming beliefs and normalize the culture that condones nonconsensual distribution.<sup>60</sup>

CyberScan's current educational presentations include a video, titled *Teen Voices: Sexting, Relationships, and Risks*<sup>61</sup>, that likewise ignores the actions of perpetrators and treats nonconsensual distribution as the inevitable consequence of trusting others. This video features several teens sharing their feelings about nonconsensual intimate image distribution. The teens consistently talk about images "getting leaked" or getting "sent around" without acknowledging that someone chose to do this and that these nonconsensual acts are what caused the harm. While showing this kind of video<sup>62</sup> may seem like an appropriate way to share the "voices of youth", the perspectives youth provide in these kinds of videos may simply echo the victim blaming and scare tactic messaging that they receive from ill-advised educational presentations (Angelides, 2013). *Education about nonconsensual distribution must challenge the idea that this act is inevitable and, instead, assert that the culture that normalizes nonconsensual acts is changeable and that we can all help support a culture that values consent and respects bodily autonomy.* 

<sup>&</sup>lt;sup>60</sup> https://mediasmarts.ca/blog/sexting-shifting-focus-victim-blaming-respect-consent
<sup>61</sup> https://www.youtube.com/watch?v=IZwVT6WnPQY

<sup>&</sup>lt;sup>62</sup> A video with a similar problematic approach was recently created by the Nova Scotia RCMP; https://www.balifaxtoday.ca/police-beat/higb-school-students-team-up-with-remp-to-create-videos-on-dangers-ofsharing-intimate-images-video-3290301

To avoid victim hlaming/shaming and to teach youth the importance of consent and bodily autonomy, educational responses need to acknowledge that consensual image sharing is not inherently harmful (Albury et al., 2017; Karaian, 2014) and, rather, that harm occurs when images are shared without consent or within a context of coercion. As teens (and adults for that matter) often report consensually sharing images for fun or to flirt, and many images that are consensually shared remain confidential (Lee & Crofts, 2015; Steeves, 2014), nonconsensual distribution should not be normalized as the inevitable result of trusting others. Rather, scholars recommend teaching young people that, like others sexual acts, intimate image sharing must only occur when there is consent (Albury et al., 2017; Hasinoff, 2015; Shariff & DeMartini, 2015). Starting with the importance of consent, education can then focus on challenging the beliefs that might make people believe it is okay to share an image without consent<sup>63</sup> or to shame/blame a victim of nonconsensual distribution. Educators could also explain that in many of the most tragic cases of nonconsensual distribution, such as the Rehtaeh Parsons case, the harm experienced by the victim was amplified by bystanders who bullied the victim rather than offering support; Students could then brainstorm the best ways to support a victim. Young people could also brainstorm practical tips to ensure they don't share someone's image without consent (e.g. delete images after a short period so that you do not risk violating someone's privacy at a later date when you might be drunk/mad/or pressured by friends and ensure your images are not being auto uploaded to other devices or the cloud).

Although the victim responsibilizing / "anti-sexting" approach was once popular, many youth-serving organizations have since recognized that this approach is counterproductive as it leads to increased shaming and blaming of victims, can make victims less likely to seek support, does not teach the importance of consent, and does not teach youth safer-sexting tips<sup>64</sup> (Dodge & Lockhart, 2021; Fairbairn et al., 2013). There are now many resources available that CyberScan could use to provide a consent-focused approach.<sup>65</sup> Telus and MediaSmarts<sup>66</sup>, Kids Help Phone<sup>67</sup>, and Webwise,ca<sup>68</sup> all provide consent-focused education that does not shame consensual sexting. The website thatsnotcool.com provides examples (such as the image on the right) of education campaigns that instead target nonconsensual or coercive behaviour and



are meant to empower youth to "set boundaries and make informed decisions" (Fairbairn et al., 2013, p. 52). Education should also help youth feel safe reaching out for support and feel that there are ways adults can help them (e.g. CyberScan can report/remove images posted online or contact the person who shared the image to have them delete it from their device). Education should also help youth feel empowered to support a peer whose image is shared without consent (e.g. refuse

<sup>&</sup>lt;sup>63</sup> For example, recognizing that boys sometimes nonconsensually share images of girls to impress other boys, educators could help youth think critically about pressures on boys to prove their masculinity and sexual experience (Ringrose & Harvey, 2015).

<sup>&</sup>lt;sup>64</sup> Teaching youth tips to sext more safely (as with safer-sex advice) does not amount to encouraging them to sext, but rather gives them knowledge and tools to make more informed choices and to feel they can come to adults for non-judgemental support.

<sup>65</sup> https://www.youtube.com/watch?v=8pqnL2-7MwU

<sup>&</sup>lt;sup>66</sup>https://mediasmarts.ca/sites/default/files/guides/guide taking youth about forwarding sexts.pdf

<sup>67</sup> https://kidshelpphone.ca/get-info/what-sexting

<sup>68</sup> https://webwise.ca/cyber-101/sexting/

to share the image, tell the person who shared it without consent that it is not okay, tell the victim you think what happened to them is wrong and you are there for them, help the victim find additional resources or supports).

Finally, CyberScan should ensure that the education they provide corrects rather than reaffirms misconceptions about nonconsensual intimate image distribution. In the Teen Voices, Sexting, Relationships, and Risks video that CyberScan shows youth, it is implied that youth victims of nonconsensual intimate image distribution are almost always girls. Contrary to this popular assumption. Canadian research has found that teen boys are actually slightly more likely to be victims of this act than girls (Steeves, 2014). While boys and girls experience similar rates of victimization, education should discuss the discriminatory beliefs that can lead to girls being judged more harshly when their images are shared without consent.<sup>69</sup> The Teen Voices video includes youth describing this increased impact on girls (e.g. "getting busted for sexting is more embarrassing for girls than guys" and "it's so easy as a female to have your reputation thrown away"<sup>70</sup>), but it does not help youth understand and challenge the discriminatory reasons why this is the case and, therefore, simply reaffirms this as "the way it is". Educators should also challenge the idea that all cases of nonconsensual intimate image distribution end in tragedy for the victim. For instance in the Teen Voices, Sexting, Relationships, and Risks video, many of the teens express that images will be spread all over the internet and will impact your life/reputation forever: "When a nude gets leaked like, your family gonna see it, different people you don't even know screen shotting you, the picture that you sent to this one person is never going to go away, it's never going to, you're just stuck with it. [...] [your] whole body is all over the internet and now everybody's seeing [you]"71. Contrary to this worst-case scenario, in many cases nonconsensually distributed images are not made publicly available but are rather shared between youth through text or messaging apps (Walker & Sleath, 2017) and are likely to be deleted on request from a CyberScan agent, school official, or parent/guardian. Additionally, even if images are widely and publicly distributed, youth should be made aware of the many supports that can help control the spread of the images (e.g. most major social media companies will remove the image and tag it as a nonconsensually shared intimate image and Google will delist images shared without consent from its search engines) and the supports that are available to help deal with resulting harms (e.g. emotional support from school counsellors, Kids Help Phone, or CyberScan). It is important to reassure youth victims rather than sending messages that confirm the idea that they should panic and that they will be unable to ever recover from this harm (See: Image/content takedown and technological know-how).

> Recommendation #29: Education on nonconsensual intimate image distribution should avoid a victim responsibilization (i.e. anti-sexting) facus and, instead, focus on the importance of consent and badily autonomy.

Recommendation #30: CyberScan must ensure that their educational messaging challenges rather than realfirms common misconceptions about nonconsensual infimate image distribution.

<sup>69</sup> https://mediasmarts.ca/blog/sexting-shifting-focus-victim-blaming-respect-consent

<sup>70</sup> https://www.youtube.com/watch?v=IZwVT6WnPQY

<sup>&</sup>lt;sup>71</sup> https://www.youtube.com/watch?v=IZwVT6WnPQY

## LABELLING YOUTH INTIMATE IMAGES AS "CHILD PORNOGRAPHY"

CyberScan's educational presentations, like many police-led educational initiatives in Canada, tell youth under the age of 18 that they have committed child pornography offences if they have consensually and privately shared an intimate image of themselves with a peer. This framing of vouths' consensual intimate image sharing as child pornography is concerning, as the law is much less straight forward on this point than CyberScan agents seem to imply to youth. In Canada, a young person has never been convicted for sharing an intimate image of themselves with a peer (i.e. sexting), and many legal scholars believe they likely never will be / should never be (Karaian & Brady, 2020). In R v Sharpe (2001), the Supreme Court of Canada stated that youth who consensually and privately create sexual images of themselves or themselves with their partner should be excluded from child pornography offences. In Sharpe, the majority decision states that this kind of consensually made and privately held intimate image could be "of significance to adolescent self-fulfillment, self-actualization and sexual exploration and identity"<sup>72</sup>. Although this decision was made before popular knowledge of "sexting" as it is now understood (Karaian & Brady, 2020), it remains unlikely that consensual youth sexting will ever be charged as child pornography because no harm has occurred in such a case. The harm occurs when intimate images are shared without consent, and it is then that charges may be used (and have been used) against a youth who has nonconsensually shared an image of someone.

Although warnings of child pornography charges for consensual sexting are likely a wellintentioned attempt to reduce the risk of nonconsensual distribution, in practice this scare tactic approach is unlikely to reduce rates of consensual sharing; Instead, it acts to send the harmful message that victims of nonconsensual distribution have done something wrong/immoral/illegal. This messaging acts to reaffirm harmful victim blaming/shaming beliefs and can make victims of nonconsensual intimate image distribution less likely to seek support due to fears of being criminalized or judged (Cyberbullying Hurts, 2012; Dodge & Lockhart, 2021; Fairbairn et al., 2013; Naezer & Oosterhout, 2021). CyberScan agents report that parents and school officials often ask them to respond to youth who have consensually created an intimate image of themselves or have consensually shared an intimate image with a partner or friend (CS2; CS5; CS6). While CyberScan agents report that they sometimes have one-on-one discussions with these consensual image creators/sharers in which they tell them that they could be charged with child pornography offences for both of these acts, it is clear in the law that self-created and privately held intimate images are not included within the scope of child pornography offences and it is unlikely that consensual sexting will be charged as child pornography either.

Many educational resources for youth in Canada now recognize that "sexting can be a healthy way for young people to explore sexuality and intimacy when it's consensual"<sup>73</sup> and that educational responses should focus on highlighting the harm and legal consequences of acts committed *without consent*. While CyberScan's responses do not currently embrace this model, *the way in which CyberScan uses warnings of child pornography offences in response to consensual sexting does vary in forcefulness depending on the agent delivering the message*. One agent in 2016 reported using explicit warnings of child pornography offences:

<sup>72</sup> R v Sharpe, 2001 SCC 2, para 109.

<sup>73</sup> https://mediasmarts.ca/digital-media-literacy/digital-issues/sexting

"[I tell youth], if you are taking a photograph of yourself and you are under the age of 18, you've just made child pornography. If you're sharing it, you've now distributed child pornography. If someone is receiving it, they are in possession of child pornography. And those are serious criminal code offences. So we would talk to them about that. Now, between you and I, there is some discretion there with the police, but we wouldn't bring that up with the youth. If police are seeing that a girl has shared a video of herself with a boyfriend and the parents found it, you know the police aren't [going to charge her] because the harm was not there... they didn't share it with the world, they were sharing it between themselves. Yes it is absolutely illegal for them to do that, but in reality the response will be to just get them to delete and remove [the images], that would be the appropriate approach when you are dealing with that type of situation" (CS4).

Although this agent was aware that police use discretion not to charge youth for consensual acts (though was seemingly unaware of the legal precedent that complicates a straightforward reading of child pornography laws), they nonetheless explicitly threatened youth who engage in consensual acts with child pornography offences. This kind of education is likely to create anxiety for youth who have already consensually shared images, and it also sends the message that victims of nonconsensual distribution should avoid seeking support from adults as they risk criminalizing themselves. On the other hand, youth may simply tune out this message as they may know from experience that those in their school who have been found consensually sexting were not criminalized with child pornography charges.

A second agent in 2016 described taking a somewhat more balanced approach that told youth that "if you're a young person in Canada under the age of 18 and you take a naked photo of yourself, technically you're in possession of child pornography. [But if someone shares your image without consent and] you come and give us the information, you're not going to get in trouble. We are going to help you" (CS2). While this kind of explanation may be less likely to discourage victim reporting, consensual youth sexters and victims of nonconsensual distribution still hear the message that they have technically committed a criminal offence and, therefore, they may still avoid seeking adult supports. A 2020 agent explained a similar approach, "[we tell youth that] even taking a picture of themselves is illegal [...] it is technically child pornography. But I tell them the police are there to help, they are not going to charge you for trying to help, [...] if you are a victim of this they are not going to charge you with making child pornography because you took a picture of yourself' (CS5). While this approach is certainly better than the forceful use of criminal offences as a scare tactic to try to stop consensual image creation and sharing, this kind of messaging is likely to leave youth confused and uncomfortable seeking adult supports. And, again, it wrongly states that even creating and privately keeping a nude image of yourself is child pornography despite the decision in Sharpe. The complexity of child pornography laws in relation to youth's consensually shared intimate images leave CyberScan agents in a difficult spot in terms of some of their messaging. Educational messaging about youths' consensual intimate image sharing would certainly be easier if child pornography offences were clarified to more explicitly exclude consensual contexts between close in age youth: However, there is no reason to believe that consensual youth sexting will suddenly start to be charged as child pornography and, therefore, many educational initiatives for youth in Canada now discuss consensual intimate image sharing as a sexual act that, like all sexual acts, has both risks and rewards but is not

*inherently wrong or harmful.* CyberScan should consider implementing this kind of nonjudgemental and sex-positive approach to education about intimate images, as this approach is now widely recognized as the most evidence-informed approach and has been taken up by organizations such as Kids Help Phone<sup>74</sup>, Webwise.ca<sup>75</sup>, and MediaSmarts<sup>76</sup>. All of these resources discuss the many legitimate reasons a youth might choose to create or share intimate images and, thereby, create an opening to non-judgmentally discuss the risks/rewards, tools to sext more safely, and the importance of consent. These resources also all explain the details of the legal context of intimate image sharing for youth in Canada, but they highlight that close-in-age youth who share images consensually will likely not be charged as child pornographers and that what is most important is to respect the consent and privacy of others.

As much as possible, CyberSean should move away from a focus on child pornography laws. This is true even when discussing nonconsensual acts of intimate image distribution. As child pornography offences were "created to protect children from sexual exploitation" by adults, many scholars, police officers, and judges<sup>77</sup> in Canada have expressed that it is inappropriate to frame nonconsensual intimate image distribution among youth as "child pornography" (Dodge & Spencer, 2018; Shariff & DeMartini, 2015, p. 295). With the more appropriate offence of nonconsensual intimate image distribution now available to charge both youth and adults who share images without consent, it is possible to discuss the potential legal consequences of nonconsensual distribution without referring to the ill-suited and overly-stigmatizing offence of child pornography. As Segal describes in his review of the Rehtaeh Parsons case:

"Many would agree that charging youths with child pornography-related offences is an unintended use of the Criminal Code's child pornography provisions. While there is a valid debate to be had on that issue, the question no longer needs to be decisively answered in light of the new criminal offences relating to distributing or making available intimate images without consent. While the child pornography offences remain available in cases like this one, these new offences would cover most instances where young persons distribute images of a sexual nature without consent, and they are arguably a better way of addressing cases where all involved are youth" (Segal, 91).

While nonconsensual intimate image distribution can rightly be said to be "technically child pornography", there is little utility in discussing this technicality with young people when they can instead be made aware of the offence of nonconsensual intimate image distribution.

Avoiding a child pornography framing for both consensual and nonconsensual intimate image sharing among youth would be easier if the provincial government provided further clarity on how mandatory child pornography reporting requirements apply to cases among youth. Currently, CyberScan agents interpret the mandatory duty to report child pornography<sup>78</sup> to the police as including all cases of consensual and nonconsensual intimate image distribution among youth,

<sup>74</sup> https://kidshelpphone.ca/get-info/what-sexting

<sup>75</sup> https://webwise.ca/cyber-101/sexting/

<sup>&</sup>lt;sup>76</sup> https://mediasmarts.ca/digital-media-literacy/digital-issues/sexting

<sup>77</sup> R v SB et al., 2014 BCPC 0279; R v Zhou, 2016 ONCJ 547.

<sup>&</sup>lt;sup>78</sup> In cases reported to CyberScan by schools, the case is often already reported to the school resource officer by the principal, so CyberScan is not required to call police themselves (CS5).

even if there is no evidence that the images have been shared in a public manner that would put them at risk of falling into the hands of an adult who would view them for a sexual purpose. Although this duty to report was created, as were child pornography charges, to address adults who sexually exploit children, CyberScan agents explained that: "If we [...] get a call that there was a mutual relationship between youth and they exchanged images and so on, we would still have to check that that is reported to local police, and then they would deal with that whatever way they felt necessary. But I would have to make sure it was at least reported, just because that's my duty to report. I'm bound under a duty to report child pornography [...]" (CS5). CyberScan agents explained that police seem to perceive these reports of image share among youth as an unnecessary nuisance, as the reason this duty to report exists is to make police aware of a child in danger of sexual exploitation at the hands of an adult: "I do have a duty that it has to be reported to the police. Now the police most times don't do anything about it, because that's the last thing they want to do, and actually they don't want to even hear it when we have to call. The police don't want to deal with that [as child pornography] right, but I think we have that legal obligation" (CS5). Although some cases of nonconsensual distribution could include public online sharing that risks images being added to online child pornography caches viewed by adults, it seems particularly unnecessary for cases to be reported in the many instances in which images are nonconsensually distributed among a particular group of youth (via showing images to others on a phone, sending to a private group message, or texting) (Walker & Sleath, 2017) and there is little chance of images somehow ending up in the hands of an adult abuser. The duty to report should be clarified, as there seems to be no purpose to reporting images as "child pornography" in cases of consensual sexting among youth (i.e. images have remained private between youth) or in cases of nonconsensual intimate image distribution where images have not been made publicly accessible (i.e. images have been shared nonconsensually but only to other youths). Despite the challenges created by mandatory child pornography reporting policies and a complicated legal landscape. CyberScan's education materials and responses should refrain from framing this act as "child pornography" whenever possible. When youth are told they have committed child pornography or are child pornographers, it can create confusion and undue stigma<sup>79</sup> and decrease the likelihood that victims of nonconsensual distribution will seek support. The current challenges in avoiding a child pornography framing speak to the importance of gaining further clarity from the courts or federal government regarding the use of child pornography offences in cases that do not involve adult abuse of children.

> Recommendation #31: CyberScan shauld avoid framing consensual intimate image creation/sharing and nonconsensual intimate image distribution among youth as "child pornography" whenever possible.

> Recommendation #32: CyberScan (as well as police and school officials) should ensure that they fully understand the limitations on how child pornography affences can be applied, as determined in R v Sharper (2001), and recognize that these offences are ill-suited (and increasingly avoided) in legal responses to cases among youth.

<sup>&</sup>lt;sup>79</sup> See R v SB et al. (2014) for one example of the negative impacts that can come from framing youth nonconsensual distribution as child pornography

Dissummit common på en virnskon la (si) avir inness å Euromekon Distument milessett ovri vent för Dis vicess in mismanistrikkt

Recommendation #33: The provincial government should review the duty to report child pornography to determine whether the duty to report applies to cases of inlimate image sharing among youth in which there is little risk of the images being used as child pornography by an adult.

### INFORMING NATIONAL RESPONSES TO DIGITAL HARM

This report has detailed several ways in which the CyberScan unit could improve its responses to cyberbullying and nonconsensual intimate image distribution. However, the core supports provided through CyberScan's support line role (i.e. technological and emotional support for complainants) is a positive and in-demand resource. CyberScan's work in this regard should be used as a model to provide all Canadians with this kind of support line. CyberScan agents in both 2016 and 2020 asserted that a national resource akin to CyberScan is needed to allow all Canadians to receive support in response to digital harms: "Here in Nova Scotia there is a place you can call, but in other places there is nowhere that you can even call about some of this stuff. Like if you go to the police and they can't help you, well at least here you can give us a call. And we're paid to research and kind of see how we can help, so it's a start and we need a lot more, but it's a start" (CS5). Some agents also asserted that a national program would allow for more comprehensive educational resources to be made available to Canadians, citing the breadth of resources available in other countries such as Australia: "Australia they have this national eSafety Commissioner and they have so many resources on there, and I wish that Canada had something like that, some sort of national organization that is there to help Canadian's have a safer experience online. [...] I'd love to be able to offer more resources and things like that if we had the money... again I just look at the site for Australia and they have [...] stuff for seniors, they have stuff for intimate image abuse, they have stuff for cyberbullying, they have stuff for newcomers" (CS5). A national strategy should allow all Canadians to access immediate emotional/informational supports and assistance with takedown/deletion of cyberbullying content and nonconsensually distributed intimate images and should also act as a hub for education, prevention, and support resources. Somewhat comparable services are available in the UK through the Revenge Porn Helpline and in Australia through the national eSafety Commissioner, but Canada does not currently have a national program to provide supports and resources. If a national support line and resources hub were to be created, it would be important to include a strategy for community-based organizations that can engage in preventative education and restorative responses in a more localized way as well. The evidence of CyberScan's successes and the recommendations for their improvement should both provide important information for the federal government as they continue to consider ways to address digital harms in Canada.

> Recommendation #34: Lessons learned from the CyberScan unit should be shared with the federal government to push for national supports that bring. Tagether the best aspects of CyberScan with additional resourcing for all Canadians.

## REFERENCES

- Albury, K., Hasinoff, A., & Senft, T. (2017). From Media Abstinence to Media Production: Sexting, Young People and Education. In L. Allen & M. L. Rasmussen (Eds.), *The Palgrave Handbook of Sexuality Education* (pp. 527–545). Palgrave Macmillan.
- Angelides, S. (2013). 'Technology, hormones, and stupidity': The affective politics of teenage sexting. Sexualities, 16(5-6), 665-689.
- Beran, T., Mishna, F., McInroy, L., & Shariff, S. (2015). Children's Experiences of Cyberbullying: A Canadian National Study. Children and Schools, 37(4), 207–215.
- Boyd, A. (2020, June 22). Should we have cops in schools? Why other districts are now asking Toronto. *Toronto Star.*
- Boyd, D. (2014). It's complicated: The social lives of networked teens. Yale University Press.
- Choo, H. (2015). Why we are still searching for solutions to cyberbullying: An analysis of the North American responses to cyberbullying under the theory of systemic desensitization. University of New Brunswick Law Journal, 66, 52–77.
- Cooke, A. (2021, May 18). Father of Rehtaeh Parsons looks to 'turn a page' in writing book about his daughter. *Global News*.
- Crofts, T., & Lievens, E. (2018). Sexting and the law. In Sexting: Motives and risks in online sexual selfpresentation (pp. 119–136). Palgrave MacMillan.
- Cyberbullying Hurts: Respect for Rights in the Digital Age. (2012). Report: Standing Senate Committee on Human Rights, Ottawa.
- Dodge, A. (2021). 'Try Not to be Embarrassed': A Sex Positive Analysis of Nonconsensual Pornography Case Law. Feminist Legal Studies, 29(1), 23-24.
- Dodge, A., & Lockhart, E. (2021). "Young People Just Resolve it in Their Own Group": Youth Perspectives on Criminal Responses to Nonconsensual Pornography. Youth Justice, Online First.
- Dodge, A., & Spencer, D. (2018). Online Sexual Violence, Child Pornography or Something Else Entirely? Police Responses to Non-Consensual Intimate Image Sharing among Youth. Social & Legal Studies, 27(5), 636-657.
- Fairbairn, J., Bivens, R., & Dawson, M. (2013). Sexual violence and social media: Building a framework for prevention. Report: OCTEVAW, Ottawa.
- Fraser, D. (October 20, 2017). Letter to Nova Scotia Legislature, Law Amendments Committee: https://nslegislature.ca/sites/default/files/pdfs/committees/63\_1\_LACSubmissions/20171023/201 71023-027-003.pdf.
- Hamilton, A. (2018). Is Justice Best Served Cold?: A Transformative Approach to Revenge Porn. UCLA Women's Law Journal, 25(1), 1–44.
- Hasinoff, A. A. (2015). Sexting panic: Rethinking criminalization, privacy, and consent. University of Illinois Press.
- Henry, N., Flynn, A., & Powell, A. (2018). Policing image-based sexual abuse: Stakeholder perspectives. Police Practice and Research, 19(6), 565–581.
- Henry, N., Powell, A., & Flynn, A. (2017). Not just 'revenge pornography': Australians' experiences of image-based abuse. Report: RMIT University, Melbourne.
- Johnson, M. (2016). Digital literacy and digital citizenship: Approaches to girls' online experiences. In J. Bailey & V. Steeves (Eds.), EGirls, eCitizens (pp. 339–360). University of Ottawa Press.
- Karaian, L. (2014). Policing 'sexting': Responsibilization, respectability and sexual subjectivity in child protection/crime prevention responses to teenagers' digital sexual expression. *Theoretical Criminology*, 18(3), 282–299.
- Karaian, L., & Brady, D. (2020). Revisiting the "Private Use Exception" to Canada's Child Pornography Laws: Teenage Sexting, Sex-Positivity, Pleasure, and Control in the Digital Age. Osgoode Hall Law Journal, 56(2), 301–349.

Khoo, C. (2021). Deplatforming misogyny: Report on platform liability for technology-facilitated genderbased violence. Report: LEAF, Ottawa.

Lee, M., & Crofts, T. (2015). Gender, Pressure, Coercion and Pleasure: Untangling Motivations for Sexting Between Young People. *The British Journal of Criminology*, 55(3), 454–473.

- Llewellyn, J., Archibald, B. P., Clairmont, D., & Crocker, D. (2014). Imagining Success for a Restorative Approach to Justice: Implications for Measurement and Evaluation. *Dalhousie Law Journal*, 36(2), 281–316.
- McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse. *Feminist Legal Studies*, 25(1), 25–46.
- Mishna, F., Regehr, C., Lacombe-Duncan, A., Daciuk, J., Fearing, G., & Van Wert, M. (2018). Social media, cyber-aggression and student mental health on a university campus. *Journal of Mental Health*, 27(3), 222–229.
- Mishna, F., Schwan, K. J., Birze, A., Van Wert, M., Lacombe-Duncan, A., McInroy, L., & Attar-Schwartz, S. (2020). Gendered and Sexualized Bullying and Cyber Bullying: Spotlighting Girls and Making Boys Invisible. *Youth & Society*, 52(3), 403–426.

Mishna, F., & Van Wert, M. (2015). Bullying in Canada. Oxford University Press.

- Morrison, B. (2002). Bullying & Victimisation in Schools: A Restorative Justice Approach. Trends & Issues in Crime & Criminal Justice, 219, 1–7.
- Naezer, M., & Oosterhout, L. van. (2020). Only sluts love sexting: Youth, sexual norms and non-consensual sharing of digital sexual images. *Journal of Gender Studies*, Online First.
- Palmeter, P. (2017, October 20). Privacy lawyer who challenged cyberbullying law worries new bill swings too far. CBC.

Powell, A., & Henry, N. (2017). Sexual violence in a digital age. Palgrave Macmillan.

- Reynolds, A. (2021, March 22). Indigenous women from across Mi'kma'ki fighting back against men sharing their images without consent. SaltWire.
- Ringrose, J., & Harvey, L. (2015). Boobs, back-off, six packs and bits: Mediated body parts, gendered reward, and sexual shame in teens' sexting images. *Continuum*, 29(2), 205–217.
- Russell, S., & Crocker, D. (2016). The institutionalisation of restorative justice in schools: A critical sensemaking account. *Restorative Justice*, 4(2), 195–213.
- Segal, M. (2015). Independent Review of the Police and Prosecution Response to the Rehtaeh Parsons Case. Report: Murray D Segal Professional Corporation.
- Shariff, S., & DeMartini, A. (2015). Defining the Legal Lines: EGirls and Intimate Images. In J. Bailey & V. Steeves (Eds.), *EGirls*, *eCitizens* (pp. 281–305). University of Ottawa Press.
- Steeves, V. (2014). Young Canadians in a wired world, phase III: Sexuality and romantic relationships in the digital age. Report: MediaSmarts.
- Taylor, J. (2016). Minding the gap: Why and how Nova Scotia should enact a new cyber-safety act. *Canadian Journal of Law and Technology*, 14, 157–171.
- Tutton, M. (2018, July 5). New cyberbullying law can force removal of intimate images online. CBC.

Vitale, A. (2017). The End of Policing. Verso.

Wachtel, T. (2016). Defining Restorative. Report: International Institute of Restorative Practices.

Walker, K., & Sleath, E. (2017). A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. Aggression and Violent Behavior, 36, 9–24.

From:	Jeff Brown (NE.ACCESS TO IN	11
To:	ICN / DCI (PCH)	
Subject:	Have your say: The Government's proposed approach to address harmful content online	
Date:	September 23, 2021 4:49:19 PM	

Hello Canadian Heritage,

This is nothing more than pure censorship. While I agree that hate and child pornography needs to be removed as much as possible, this new framework is far too loose so that virtually anything the government deems "harm" would be included and it will eliminate free speech. Free speech has been almost fully removed now from most platforms and the legitimizing of this via this bill would be the death stroke of our society.

This framework should not be put forward and our society should have the freedom to police itself on what it finds acceptable or not.

I am 100% against this bill.

Jeff Brown

s.19(1)

 From:
 Mark Akrigg

 To:
 ICN / DCI (PCH)

 Subject:
 The harmful content proposal is itself extremely harmful

 Date:
 September 24, 2021 6:58:22 PM

In 2007 I founded Project Gutenberg Canada (gutenberg.ca), a popular website which offers free digital editions of books in the Canadian public domain. I am shocked by the draft proposals, which certainly open the door to illegal takedowns of websites such as gutenberg.ca. I fully agree with what OpenMedia says in the attached petition which they have been promoting, and with which I fully agree.

I also think that cooperation with the other federal parties can only do good.

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Dr. Mark Akrigg Founder, Project Gutenberg Canada

s.19(1)

From:	the A
To:	ICN / DCI (PCH)
Subject:	The government"s proposed approach to address harmful content online
Date:	September 24, 2021 6:15:12 PM

To Whom It May Concern,

While I am neither a Canadian nor a sex worker myself I know many sex workers and am concerned about the implications of this new policy on sex workers as a whole as well as the health and freedom of the internet.

The United States implemented a similar policy in FOSTA/SESTA which has been widely evaluated as ineffective in it's original aims and disastrous to sex workers.

I urge the government to reconsider this new policy. Thank you.

Sincerely,

Aidan Kahrs

Sent with ProtonMail Secure Email.

### Felicia Mazzarello

From: Sent: To: Subject: Ugo Gilbert Tremblay September 24, 2021 12:44 PM ICN / DCI (PCH) Question

s.19(1)

Bonjour,

J'envisage de vous faire parvenir mes commentaires relativement à l'initiative du gouvernement pour lutter contre le contenu préjudiciable en ligne et j'aimerais savoir quelle est la date limite pour participer.

En vous remerciant,

Ugo Gilbert Tremblay (LL. D., Ph. D) Chercheur postdoctoral Faculté de droit, Université McGill

Wendy Hayhoe
ICN / DCI (PCH)
Online Harms Consultation
September 24, 2021 5:19:35 PM

In response to your public consultation, I would like to ask for the following:

- Please ensure that sites which frequently host CSAM and/or intimate images shared without consent do not receive criminal immunity from past offenses and will be held criminally responsible if they do not comply with the regulatory demands
- Please require sites to take robust proactive measures to prevent uploading CSAM and/or intimate images shared without consent, including verifying the age & consent of all those depicted prior to hosting content
- Please adopt the proposed changes to strengthen the Mandatory Reporting Act by incorporating option #2, which requires user's basic subscriber information. This would allow law enforcement to locate offenders and rescue victimized children faster.

Thank you for the opportunity to provide feedback.

Sincerely, Wendy Hayhoe

s.19(1)

## Felicia Mazzarello

From: Sent: To: Subject: Heather Jarvis s.19(1) September 24, 2021 6:34 PM ICN / DCI (PCH) Concerned about Digital Citizen Initiative harmful online approach

Dear Heritage Canada,

I want to have my day and share my concerns over the proposed initiative regarding digital harms. I echo and emphasise Safe Harbour Outreach Project's (SHOP) letter outlining why this framework is overreaching, overly broad, and if it moves forward as is will inevitably target sex workers safety, 2SLGBTQIA education and content, BIPOC advocacy and online content, harm reduction information online, and online sexual speech and sex education.

Please listen to the many people bringing forward concerns about this initiative, including SHOP's letter here: <a href="https://sjwomenscentre.ca/wp-content/uploads/2021/09/SHOP-letter-in-response-to-digital-harms-Cdn-gov-Sept.242021-PDF.pdf">https://sjwomenscentre.ca/wp-content/uploads/2021/09/SHOP-letter-in-response-to-digital-harms-Cdn-gov-Sept.242021-PDF.pdf</a>

Please reconsider these measures and heed the expertise of the marginalized communities that would be most directly targeted by these kinds of digital legislative frameworks in drafting safe, more effective alternatives.

Sincerely, Heather Jarvis

"Be kind, for everyone you meet is fighting a battle you know nothing about."

 From:
 Ashwin Sira

 To:
 ICN / DCI (PCH)

 Subject:
 Digital Citizen Initiative Feedback

 Date:
 September 24, 2021 5:31:22 PM

Hello, this is my feedback for the new proposed harmful content legislation: https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html

I can see the good intent behind this, however the approach laid out here introduces some dangerous mechanisms which could be misused. I **do not** want to see this legislation introduced. My two main points are:

- 1. Disempowering users
- 2. Potential for abuse

**Disempowering Users:** 

When it comes to disempowering users, the constant message I see is that users on the internet are completely helpless in the face of harassment and bullying online. This leaves out the fact that every platform has functions to block and report bad users. The blocked user is no longer able to communicate, and can be flagged for action by platform moderators.

There are gaps in harassment laws where people make alt accounts to circumvent these blocks and bans which could be improved.

When discussing this topic many of my less tech-savvy friends had **no idea these block and report functions existed**. A campaign to educate the general public on actions they can take on their own empowers them to simply block bad actors and report them to platform moderators for further action. Users who do not feel helpless can more actively work to build better online communities.

### Abuse Potential:

The definitions of "terrorist" and "harmful" content seem somewhat loose. I can see this easily being twisted to go after activists and organizations for purely political purposes. In theory a remedy exists in the courts, however that mechanism is slow. Events south of the border show just how quickly things can go sideways. If a bad political actor abused these tools to supress dissent on a critical issue a resolution through the courts could come far too late.

### Conclusion:

I see the good intent behind C-36, but the potential for abuse is massive. I've been the recipient of racism and abuse both in the real world and online. The online abuse never bothered me, because it has a literal off switch. Educating the general public about basic blocking and reporting functions that are standard on every online platform empowers users

to delete this garbage from their online lives.

The unfortunate part of living in a free democracy is having to deal with this sort of junk. I'd rather have to deal with that than have these tools in the hand of a bad political actor who has no qualms about abusing them for personal gain. Democracies have fallen before, and believing it simply can't happen to us or that these tools will never be abused is beyond arrogant. Even if the courts reversed a bad decision, it could be far too late.

Feel free to contact me if you would like to discuss any of these points.

Thanks!

Ashwin Sira

 From:
 Rena Kunisaki

 To:
 ICN / DCI (PCH)

 Subject:
 "harmful content proposal" is harmful indeed

 Date:
 September 24, 2021 3:32:12 PM

Just because Canada's internet is comparable to that of a third world country doesn't mean we need to go all the way and censor it like one.

All this kind of thing achieves is pushing crooks to use stronger encryption, making sites not want to serve us because of the red tape involved, making people distrust the government (why trust someone who clearly doesn't trust them?) and destroying privacy, security, and reliability online.

It definitely won't stop crime, disinformation, or abuse, just as it hasn't anywhere else. It will only turn the whole internet into YouTube - a place where mentioning certain words, subjects, or events, or doing something that a computer mistakes for pornography, gets you silenced - and many of these forbidden words aren't told to you even after you've used them. A place where original content is frequently removed, or its creators punished, because someone falsely claimed it used their music without permission. A place that remains popular only because of inertia.

I'm sure that's exactly the plan, but I'll add one more to the count of people opposing it anyway.

From:	Paul V
To:	ICN / DCI (PCH)
Subject:	Comment on proposed regulations for social media companies
Date:	September 24, 2021 1:04:26 PM

#### Hello,

I am excited to see the Government of Canada taking strong action against the proliferation of harm done online. I have reviewed the categories of harm and found them to be reasonable as a first step. I do believe that applying these in a regulatory context instead of criminal is an effective and sensible way to reduce harm. As a voter in Vancouver BC, I support this proposal in its entirety and would consider support for this essential in my representatives.

Thank you, Paul Vorvick

From:	Lisa Whitsitt
To:	ICN / DCI (PCH)
Subject:	Online Harms Consultation
Date:	September 24, 2021 2:30:02 PM

#### Hello,

In response to your request for input from the public regarding the proposed online harms legislation I would like to share a few thoughts regarding 2 of the harms: CSAM and the non consensual sharing of intimate images.

Currently, there are numerous businesses that use social media platforms to share pornography. Many of those in the pornographic videos are either under the age of 18 or adults who have not given consent. I feel that these companies are not following the Mandatory Reporting Law and may only report a small handful of videos when there are millions of videos on their sites that are illegal. I think your proposed changes to strengthen the Mandatory Reporting Act are excellent. I would like to see that option 2 be implemented so that a user's basic information is available making it more effective and faster for law enforcement to act on the sharing of CSAM and rescuing victimized children.

I also feel that age verification and consent should be required by every actor in a pornographic video to prevent victimization of adults and the making of CSAM and its illegal uploading to social media platforms. Age verification should also be required for those who use adult themed platforms so that children do not have access to this material

For many years, pornographic websites and social media platforms have escaped being held criminally responsible for their hosting of CSAM and non-consensual image sharing. It is imperative that these companies and individuals are held accountable for breaking the law and do not receive criminal immunity from past offenses.

Lisa Whitsitt

s.19(1)

From:	Robert E. Rutkowski
To:	pm@pm.gc.ca; justin.trudeau@parl.gc.ca; ICN / DCI (PCH)
Cc:	Erin.OToole@parl.gc.ca; jagmeet.singh@ndp.ca; info@bloc.org; governance@greenparty.ca
Subject:	Canada's online censorship plan endangers free expression
Date:	September 24, 2021 1:36:00 PM

Right Honourable Justin Trudeau Office of the Prime Minister 80 Wellington Street Ottawa, ON K1A 0A2 Fax: 613-941-6900 Email: pm@pm.gc.ca, justin.trudeau@parl.gc.ca

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St Gatineau QC K1A 0S5 pch.icn-dci.pch@canada.ca

Re: Canada's online censorship plan endangers free expression

Dear Prime Minister:

The Canadian government should ensure its plan to address harmful content online complies with international human rights standards. The current online censorship proposal is an attack on freedom of expression.

To protect the rights of people at risk, the following issues with the proposal should be addressed:

overly broad categories of speech that could be removed, a 24-hour takedown requirement once content is flagged, proactive filtering or monitoring obligations by online communications services,

severe penalties for non-compliance with the law, and government-mandated content removal.

Canada's framework to censor speech online is an assault on freedom of expression. The proposal would result in broad content takedowns, gutting the Canadian people's ability to hold power to account. This is especially problematic for people of color and other marginalized voices, who already experience censorship online for speaking out against injustice.

Read Access Now's full comments:

https://www.accessnow.org/cms/assets/uploads/2021/09/Access-Now-Canada-Online-Harms-Proposal-Comments-Final-09232021.pdf

Yours sincerely, Robert E. Rutkowski

cc: Erin O'Toole Leader of the Conservative Party of Canada 1720-130 Albert Street

Ottawa ON K1P 5G4 Tel: 613-755-2028 1-866-808-8407 Fax: 613-755-2001 Email: Erin.OToole@parl.gc.ca

Jagmeet Singh Leader of the New Democratic Party of Canada 300-279 Laurier Avenue West Ottawa ON K1P 5J9 Tel.: 613-236-3613 Fax: 613-230-9950 jagmeet.singh@ndp.ca

Yves-François Blanchet Leader of the Bloc Quebecois 402-3750 Crémazie Boulevard East Montréal QC H2A 1B6 Tel.: 514-526-3000 1 888 448-1880 (Sans frais) (514) 526-2868 info@bloc.org

Annamie Paul Green Party of Canada 116 Albert Street, Suite 812 Ottawa, Ontario K1P 5G3 governance@greenparty.ca

2527 Faxon Court Topeka, Kansas 66605-2086 USA P/F: 1 785 379-9671 E-mail: r\_e\_rutkowski@att.net

From:	Vivian Duperron
To:	ICN / DCI (PCH)
Subject:	Grave concerns with the Digital Citizen Initiative Technical Paper
Date:	September 24, 2021 3:32:08 PM

Hello,

I'm writing to provide comment on the technical paper under 'Have your say' at https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html.

While I recognize the premises in section 1, I believe that many parts of the paper are flawed and will result in unintended issues.

If such an act had been around sixty years ago, many of society's counterculture movements would have been quashed. And that's what this promises to do in the future. The act is not necessary and should not be entertained at all by the government. However, if such an act must be passed, my recommendations are below.

My proposals are:

For 2, the paragraph should be amended so that the Act should define the term OCS as a service that provides auto-curating (as all of the examples in the discussion guide to), or at least clarify 'private communications'.

For 3, it should require an act of Parliament to include a new category.

For 8, I disapprove of the regulatory context expanding from the criminal code. It should be criminal if it must be, or not controlled by the government.

For 10, this is 100% going to result in overmoderation, and is significantly broader than any other first-world country has done. If the act is going to mandate this along with 'reasonable measures', it should also require that automated removals be reviewed by a human and feedback provided to the individual who has been censored by the order of the Government of Canada.

For 11, the act should prescribe a method for challenging such a takedown.

16. Why should the act ensure the OCSP may not seek advice on specific decisions, given that the Government is forcing them to make it in the first place?

19. Do not entrust one person with the ability to increase the amount of material subject to this. Any expansion of categories should require a notice-and-comment period.

20. The act should *not* require notification to the RCMP, particularly on grounds of suspicion. The act should instead require a clear process for the RCMP to obtain a court production order upon the RCMP reporting content which falls within the 5 categories.

26. Should be inverted - The act should provide the OCSP \*must\* disclose that it has reported an individual to the government for their illegal speech. If the government's right to secretly investigate someone must be paramount, then the act must provide such notice after an appropriate amount of time.

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act.

31. Should be struck. Removing any downside to getting it wrong severely biases overreporting of innocent individuals.

42. The act should punish complaints made in bad faith, otherwise there's no downside to making them.

54. This results in the content not being made accessible. Material made inaccessible should be made accessible again while the Digital Resource of Canada is considering it and pending its result, with a potential carveout for individuals who have unsuccessful challenges in the past.

89. Is extremely sweeping. This should require a court order.

92. Do not compel acts

120. There is no precedent for this, and if such capability is built it will be repurposed for increasingly more and more in short order. The entire 'Exceptional Recourse' section should be struck, and introduced as a separate piece of legislation, if *and only if* it is necessary.

Module 2:

7 and 8 should be struck - the RCMP have no issue obtaining court orders for that information now, and the normalization of providing information to the government without court orders should not be furthered. Stop trying to short-circuit the courts for this.

Overall, I think the entire piece of legislation should be struck. The harms it can do far exceed the potential benefits.

Thank you, Vivian

s.19(1)

Re: The Government's approach to address harmful content online Submitted by: Rose A. Dyson Ed.D. President: Canadians Concerned About Violence In Entertainment Vice President: World Federalist Movement of Canada: Toronto Branch Author: *MIND ABUSE Media Violence And Its Threat To Democracy* (2021) email: <u>rose,dyson@alumni.utoronto.ca</u> or <u>rdyson@oise.utoronto.ca</u> Phone: 416-961-0853 or 647-382-4773

Dear Committee Members

Thank you for the opportunity to participate this discussion on meaningful action to combat hate speech and other kinds of harmful content online. Public concern about harmful media content has now been with us for several decades and the need to address the problem has gotten increasingly urgent. The five categories identified as hate speech and other kinds of harmful content online, including child sexual exploitation, terrorist activity, content that incites violence, and the non-consensual sharing of intimate images have skyrocketed as communications technologies have evolved.

As far back as 1975 Judy La Marsh, a lawyer, journalist and former member for the Liberal Government of Canada was appointed by the Government of Ontario to chair the Royal Commission on Violence in the Communications Industry. It was empowered to study the effects on society of increasing violence in the media of the day and make appropriate recommendations on measures to be taken by different levels of government, by industry and the public at large. Most of the 80 plus recommendations have never been implemented. Some have been repeated in subsequent studies but still not implemented.

In my doctoral thesis, completed at OISE/UT in 1995, I reviewed the research findings conducted by the La Marsh Commission and other studies done up until that time, subsequent recommendations and evidence or lack thereof regarding implementation. Two books on the subject followed. The first published in 2000 and the second earlier this year. A complimentary copy of either one is available upon request. The latest is titled, *MIND ABUSE Media Violence And Its Threat To Democracy*, (2021) Over the past 30 years I have watched the problems mushroom with increasing evidence of commercial reliance on themes of sex and violence in media production. In addition we have had fading boundaries between different forms of media. These include news, fiction, advertisements and educational programming, leading to catch phases such as edutainment and infotainment.

Digital technologies and the internet have magnified the problems with policy makers loath to take on the challenge of much needed and overdue regulation, frequently to avoid accusations of censorship. Inadequate distinctions between individual freedom of expression and corporate freedom of enterprise have persisted. Periodic studies funded by industry are released into the public domain countering evidence of harmful effects thus ensuring no interruptions to business as usual. For decades the cultural industries have been given carte blanche to determine what we see, hear and read.

In 1996, along with 250 other scholars and media activists representing over 88 organizations

from around the world, I helped the late George Gerbner, an internationally renowned media scholar, launch the Cultural Environment Movement at Webster University in St. Louis. That Convention was preceded by the International Summit on Broadcast Standards attended by Keith Spicer, then chair of the CRTC and other Canadians representing business and non-profits. In his work, Gerbner frequently referred to violence creep in popular culture and other forms of media, including news and advertisements, as the hidden curriculum for a Mean World Syndrome.

My colleague, retired U.S. Lte. Col. David Grossman, a psychologist and Military Expert, has written 5 books on the subject of violent first person shooter video games and the dangers of indiscriminately marketing these games to the youngest most vulnerable people on the planet. In his latest book, *Assassination Generation Aggression, Video Games and the Psychology of Killing* (2016) he provides chilling detail on how these have led to mass murders and fueled terrorism. Grossman reveals how violent video games have ushered in a new era of mass homicides worldwide. The trends have led to what he calls Acquired Violence Immune Deficiency Syndrome.

The kind of online hate and extremism that led to the January 29, 2017 mass murders at the Centre culturel islamique de Quebec, and on March 15, 2019, in Christchurch, New Zealand, is inherent in the thematic content of numerous video games played by the killers. In both cases news coverage identified evidence of heavy diets of first person shooter video game playing on the part of these perpetrators. This is a pattern that is described over and over again by other researchers among them, Mark Bourrie, author of *Martyrdom, Murder and the Lure of Isis*, and Megan Condis, author of *Gaming Masculinity*, *Trolls*, *Fake Geeks*, and the Gendered Battle for Online Culture.

What must be recognized is that the Government's focus on regulating social media and combating harmful content online cannot be confined to "speech only". Violent forms of fictional entertainment such as video games depict storylines that glorify violence, hatred, anti semitism and sexual exploitation. It would be duplicitous and of marginal value to address the problems involving work place harassment, misogyny and other excesses on the internet but to leave such content in popular culture unaddressed and unregulated. Countless studies over the years have demonstrated that these fictional depictions lead to learned behaviours based on psychological conditioning that result in distorted value systems, a tendency to resort to violence as a conflict resolution strategy, addiction and feelings of victimization, among other harmful effects.

It has also been demonstrated that violent, first person shooter video games provide fertile soil for sowing the seeds of resentment among young vulnerable white males. An "us versus them" mentality is encouraged, helped along by social media algorithms that capitalize on our genetic tendencies to respond quickly to negative themes. It has also been reported that white supremacist groups watch the latest releases of video games that are most amenable to their purposes of recruitment. Some have taken to producing their own.

The work being done by technology experts like the Institute of Electric and Electronic Engineers (IEEE) on a roadmap for 5G and global integration to facilitate the more efficient use

of energy must also focus on the nature of energy use. Spokesmen on behalf of the Institute now stress that more efficient use of what is rapidly becoming unsustainable energy demand on the internet is essential and required to reduce both collective and individual carbon footprints. But, clearly, emphasis on discretionary use is also required. Assuming we are put on a war time footing, as advocated by Seth Klein in his book, *A Good War: Mobilizing Canada For The Climate Emergency* (2021), rationing of internet use will have to be adopted. In December, 2020, Nicholas Kristoff wrote in the *New Yor k Times* that Pornhub, owned by Mindgeek in Montreal, was the third most visited and influential website on the Internet. It is inconceivable, in a world focused on sustainability and transitioning to clean energy that, on the Internet, harmful excesses are overlooked and excused as essential components to be protected under the umbrella of civil liberties. Surely the expertise in electronic engineering should not be misdirected in the race against time to ensure internet use that fosters social harm.

There are also concerns expressed by health advocates, such as Devra Davis, author of DISCONNECT The Truth About Cell Phones, What the Industry Has Done To Hide It and How To Protect Your Family (2010), about harmful radiation from digital devices that can cause cancer. In this context it behooves the government to take note of the recent United States Court of Appeals for the District of Columbia Circuit judgement in favour of environmental health groups. It found the Federal Communications Commission (FCC) in violation of the Administrative Procedures Act for not responding to comments on environmental harm. In short, the FCC failed to respond to record evidence that exposure to low level radiation from digital devices may cause negative health effects

#### Re: Strategy to combat hate speech and other harms:

We endorse the move to amend the Canadian Human Rights Act to enable the relevant Commission and Tribunal to review and adjudicate hate speech complaints.

- \* But, over reliance on industry, itself, to monitor social media content, has proven in the past to be an exercise in futility. One minor exception involves the Canadian Broadcast Standards Council which was set up in 1993 by the Canadian Association of Broadcasters to respond to complaints of inappropriate content on radio or television programming. This Council could be expanded or duplicated to monitor online content. However, the Council has always been reactive rather than proactive with no oversight for industry excesses unless complaints arise from the public at large. That needs to change. Allowing the fox to guard the henhouse with no government oversight has never worked.
- \* Second, definitions of obscenity and sections on child pornography need to be updated and expanded. Research conducted in the latter part of the last century, demonstrates how all pornography can be addictive. In addition it involves social learning theories that lead to themes of aggression and dominance. These tendencies can trickle down to the most vulnerable targets of exploitation which are children. Before the bill on child pornography, making possession, production and distribution a crime was passed in 1993, considerable attention was paid by the Government's Standing Committee on Culture and Communications set up at that time. It came out with a number of additional recommendations that were never implemented. One of them was to determine the

criminal legislative measures needed to include extremely violent forms of entertainment in the Criminal Code in ways that would conform with the *Charter of Rights and Freedoms*. See *MIND ABUSE Media Violence In An Information Age* (Dyson, 2000).

- \* The objective to authorize the Government to include or exclude categories of online communication service providers from the application of the legislation within certain parameters is important but there must be complete transparency on how this will be done and who will provide expert advice on these parameters. Advice must be sought from health providers and other researchers not beholden to industrial interests.
- \* Film and video game monitoring of media content for entertainment purposes is now undertaken by provincial classification boards. A national system would be much more efficient. While great care has been taken over the years to ensure gender and racial diversity on most boards the overall tendency has been for them to bend to the will of industry. Criteria on what is age appropriate should involve input from child development experts. This has yet to happen. Indeed, the prevailing standard for most classification boards throughout the developed world has been set by the industry funded and operated, Hollywood based Motion Picture Association of America. That needs to change.
- \* Legislation should be passed on a national level to ban advertising to children 13 years and under. Such legislation has been in effect in Quebec for over 25 years. Occasional bills for implementation have been introduced from time to time in Canada at the national and provincial levels of government, boards of health and in 2016 even an editorial in *Globe and Mail*, called for one. Most developed countries have already adopted this kind of legislation, citing various concerns, among them, protecting children from harmful sexual exploitation, violent content, all advertising, the marketing of junk food known to cause physical health problems such as obesity and heart disease and the dangers of exposure to low level radiation from the internet.
- \* The Committee must not allow itself to be intimidated by industry push back. On January 14, 2019, it was reported in *The Globe and Mail*, that a proposal from Health Canada to amend the Food and Drug Act by restricting food and beverage marketing to children had hit a familiar snag: industry protests that such regulation was "unrealistic", "punitive" and "commercially catastrophic". The huge jump in commercial exploitation of children in recent decades is nothing short of tragic. According to the Harvard Medical School founded, Boston based, Campaign for a Commercial-free Childhood, over \$17 billion was spent by the industry in 2006 in the U.S. alone to market products to children, a staggering increase over \$100 million spent in 1983. Over \$500 billion in purchases annually by that time was estimated to be influenced by children under the age of 12 years. These trends are clearly at odds with efforts focused on reducing consumer driven habits to facilitate future sustainability.
  - A very popular solution for dealing with harmful media has always been better vigilance

from parents, along with media and digital literacy taught in schools by teachers. Although it is obvious that the problem is too big and pervasive and that better cultural policy is also urgently needed, there is room for improvement in the provision of reliable, fact based educational resources. Over the years there has been increasing evidence of subtle, industry friendly resources creeping into school curriculums on the subject. In 1975, the La Marsh Commission recommended that an Advisory Board of educators, health professionals and parents be established at the Ontario Institute for Studies in Education at the University of Toronto for the provision of public education. I reiterated the recommendation in my doctoral theses completed at the Institute in 1995, and again in my two subsequent books on media violence. Nevertheless, it has yet to be established. Better government funding and support is also needed for NGOs, such as Internetsense First, founded by Charlene Doak Gebauer, which now provide urgently needed help to parents and teachers on digital supervision.

- \* Funding that is independent of industry donors, should be mandatory to ensure accuracy in monitor media violence and other harmful trends on the internet. Important models were established at the Annenberg School of Communication, University of Pennsylvania and Temple University in Philadelphia, by the late George Gerbner. The Cultural Indicators Model, later expanded into the "Fairness" Indicators Model and used by Paquette and de Guise at Laval University in Quebec City in their study Index of Violence in Canadian, Television done in 1994, is one example.
- \* An Act respecting the mandatory reporting of Internet child pornography by persons who provide an internet service is needed. But it is not clear how this would interface with the Mandatory Reporting Act.
- \* New legislation requiring regulated entities to monitor harmful content through the use of automated systems based on algorithms would be a useful way to use the new technology for prosocial purposes, given the widespread evidence of how algorithms are currently employed solely for the purposes of financial gain and fostering errant behaviour.
- \* Now, within universities across Canada and beyond, there is growing emphasis of courses offered in esport involving first-person shooter video games. This is counter productive to advocacy from experts calling for critical thinking skills, media and digital literacy and studies which point to harmful effects. There has also been ample evidence reported in *The Globe and Mail*, of generous subsidies given to video game industries such as *Ubisoft* without any regard for the nature or content involved in the productions. Tax breaks and subsidies for harmful video game production and distribution is no more justifiable than breaks for fossil fuel industries in a time of climate crisis. As pointed out by *Globe and Mail* business reporter Scott Barlow, this poses a moral dilemna (Barlow, October 14, 2017). Furthermore, these must also not be excused or spun by industry pundits as "funding for electronic arts".
- \* It is stated that regulated entities would be required to notify law enforcement in instances where there are reasonable grounds to suspect imminent risk of serious harm to any person or property from potentially illegal content falling within the five categories of

harmful - terrorist content; that which incites violence; hate speech; non-consensual sharing of intimate images; and child sexual exploitation. But it is stated that there would be no obligation to report such content to law enforcement or CSIS. Why not?

- \* And why would the threshold for such reporting of potentially terrorist and violent extremist content be lower than that for potentially criminal hate speech?
- \* The proposed legislation for a new Digital Safety Commission of Canada to support three bodies that would operationalize, oversee and enforce the new regime sounds promising. But who exactly would sit on the final stage of recourse on the Recourse Council? Diverse expertise and membership that is reflective of the Canadian population is essential to avoid having such a Council stacked with former or retired officials sympathetic to the concerns of industry. This would necessitate expertise from the health and social sciences. Transparency in public reporting obligations would also be required.
- \* An Advisory Board that would provide both the Commissioner and the Recourse Council with expert advice must include more than expertise on emerging industry trends, technologies and content-moderation standards. Who would be expected to provide information on "content-moderation standards". Like the recommended advisory group for parents and teachers, with funding independent of industry sources and the Recourse Council, such a Board should include social science expertise and input from both physical and mental health experts. Having the Digital Safety Commissioner of Canada mandated to lead and participate in research and programming, convene and collaborate with relevant stakeholders and support regulated entities in reducing the five forms of harmful content will only work if input is not confined to industry related interests. Again, the composition of the Advisory Board must include, along with all the other stakeholders itemized, health expertise.

## **Re: Compliance and enforcement**

\* The powers of the Commissioner are necessary and sound reasonable.

# Re: Modifying Canada's existing legal framework including the Canadian Security and Intelligence Act (CSIS)

\* Centralizing mandatory reporting of online child pornography offences through the RCMP's National Exploitation Crime Centre to ensure stronger requirements for internet service providers for reporting excesses would help but continuing vigilance to ensure that is happening must be provided. Not requiring judicial authorization in reports to law enforcement is necessary to expedite police response in cases where an offence is clearly evident. The same criteria should be applied to CSIS to ensure more timely access to relevant information that could help mitigate the threat of online violence extremism. For this process to take 4-6 months, as it does now, seriously diminishes their capacity to be effective.

Again, thank you for the opportunity to participate in this timely discussion. If provision is made

for appearance via zoom before the committee to submit a statement I would appreciate the opportunity.

**References:** 

Barlow, S. (2017b, October 24) Getting hooked on gaming stocks. The Globe and Mail. P.B6.

Barlow, S. (2017a, October 14) As investing theme video games score big. *The Globe and Mail.* P.B3.

Bourrie, M. (2016). The Killing Game: Martyrdom, Murder and the Lure of ISIS. Toronto, ON: Harper Collins Canada

Condis, M. (2018) Gaming Masculinity: Trolls, Geeks and the Gendered Battle for Online Culture. Iowa City, IA: University of Iowa Press.

Davis, D. (2010). The TRUTH About Cell Phone RADIATION: What the INDUSTRY has Done to Hide It, and How to PROTECT Your FAMILY. New York: Dutton.

Doak-Gebauer, C. (2019) THE INTERNET: ARE CHILDREN IN CHARGE? Tellwell, Canada.

Dyson, R. A. (2000). *MIND ABUSE: Media Violence in an Information Age*. Montreal: Black Rose Books.

Dyson, R.A. (2021). MIND ABUSE: Media Violence and its Threat to Democracy. Montreal: Black Rose Books. UT Press, AMAZON

Grossman, D. (2016). ASSASSINATION GENERATION: Video Games, Aggression and the Psychology of Killing. Boston, MA, Little, Brown & Company.

Klein, Seth. (2021). A Good WAR: Mobilizing Canada For The Climate Emergency. Amazon: U.S.

United States Court of Appeals for the District of Columbia. EHT Victorious in Federal Court Case Against FCC on Wireless Radiation Limits. August 14, 2021.

# Felicia Mazzarello

From:	Dave Poitras <dave.poitras@inspq.qc.ca></dave.poitras@inspq.qc.ca>
Sent:	August 16, 2021 3:35 PM
To:	ICN / DCI (PCH)
Subject:	Questions concernant consultation

Categories:

Alyssa

Bonjour,

Étant donné le déclenchement des élections fédérales, je me demandais si votre consultation sur l'Approche proposée par le gouvernement pour s'attaquer aux contenus préjudiciables en ligne était toujours en cours.

Si oui, je me demandais sous quelles formes nous pouvions vous faire parvenir nos « commentaires » et nos « observations ». S'agit-il, par exemple, d'un mémoire, ou vous vous attendez à un document plus succinct.

Au plaisir,

Dave Poitras, Ph.D.

**Conseiller scientifique spécialisé** Sécurité, prévention de la violence et des traumatismes Direction du développement des individus et des communautés Institut national de santé publique du Québec

Professeur associé Département de sociologie Faculté des arts et des sciences Université de Montréal

### Felicia Mazzarello

From: Sent: To: Subject: Philip Palmer August 16, 2021 1:03 PM ICN / DCI (PCH) Internet Harms: The Proposed Digital Safety Commission

At paragraph 60 of the Technical Paper, the establishment of a Digital Safety Commission ("the Commission") is proposed. I am having trouble understanding both the nature of the Commission and the relationship between the Digital Safety Commissioner ("the Commissioner"), the Digital Recourse Council ("the Counsel") and the proposed Digital Safety Commission .

First, the Commission doesn't seem to be a Commission. There is no reference to a number of people constituting the Commission or the method of their appointment. There is reference only to an Executive Director appointed by the Governor in Council. Is this correct?

Second, is the Commission really just a secretariat to the Commissioner and the Council?

Third, will the Commissioner and the Council have direct employees, or will those be under the employment of the Commission?

Fourth, will the Commissioner or the Council have the power to direct the activities of the Commission?

I would appreciate your help in understanding more precisely the functions and operations of the proposed Commission. Feel free to call me if that would be most convenient to you.

With thanks in advance,

s.19(1)

Yours very truly,

Philip Palmer

#### Felicia Mazzarello

From: Sent: To: Subject: cris fraenkel August 12, 2021 1:07 PM ICN / DCI (PCH) Re:

Categories:

Cathy

To add to my previous.... here's a recent example of a Canadian journalist getting censored by YouTube's automatic filters, for saying the **\*\*OPPOSITE\*\*** of what the filters were attempting to censor.

https://taibbi.substack.com/p/meet-the-censored-paul-jay

These examples show up almost daily, and that's just the ones that get noticed and written about. You can be sure there are 100s more that don't get noticed for every one that generates press coverage.

s.19(1)
On Wed, Aug 11, 2021 at 9:55 PM cris fraenkel < wrote:

I am commenting on the governments plan to empower internet providers to become the next supercharged police force online.

Specifically, your request for comments here: <u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html</u>

You are taking a well intentioned attempt at solving a relatively small, relatively isolated problem, but using an approach that will cause our whole society much more harm than the problem you're trying to fix.

Specifically

- your arbitrary 24 hour deadline for taking action ensures no chance of considered, human review. Reacting that fast to the huge quantity of new content can only be done by automatic filters. Every time this has been attempted, it has failed miserably.... examples include being unable critique issues because you can't talk about them without getting banned, and completely off-topic content being banned because they happened to use too many triggering words (in a different context - but algorithms can't know that)

- huge penalties for failure to remove deemed 'harmful' speech, but no penalties for removing permitted speech in error guarantees a 'shoot now, ask questions later' approach, with 'later' meaning 'never'.

- the technical difficulty and cost of meeting your requirements are a gift to Facebook, Twitter, Apple and the like. No new competitors could ever hope to compete, cementing their stranglehold on online discussion.

Do not make the problem worse (which this will do).

sincerely

Cris Fraenkel

000689

# Felicia Mazzarello

From:	Richard Yates <
Sent:	August 11, 2021 3:08 PM
To:	ICN / DCI (PCH)
Subject:	new legislative and regulatory framework that would create rules for how social media platforms and other online services must address harmful content
Categories:	PM

There is NO MEDIA coverage of this technical proposal by the government.

There is NO CONSULTATION that I can see.

Why is Trudeau & the Liberals so intent on ramming through an ill-conceived and frankly dangerous new regulations & law?

At the least, you should consider the following. These will pass for my "input" on what you are proposing!!!

Picking Up	Where	Bill C-10	Left Off:	The	Canadian	Government'	s Non-C	consultation o	n Online	Harms
Legislation										

and

O (No!) Canada: Fast-Moving Proposal Creates Filtering, Blocking and Reporting Rules—and Speech Police to Enforce Them

You aren't holding "public hearings".

You haven't publicized widely your "request for public comment".

Why are you hiding? What are you afraid of?

Why are you so intent on pushing such slapdash and truly dangerous new regulations and law???

I am:

Richard Yates

s.19(1)

### Felicia Mazzarello

From:	Richard Yates	1	
Sent:	August 11, 2021 2:57 PM		
To:	ICN / DCI (PCH)		
Subject:	new regulatory framework	s.19(1)	
Categories:	PM		

I'm writing regarding: Technical paper - Canada.ca

#### Technical paper - Canada.ca

Canadian Heritage

This technical paper on online hate summarizes the drafting instructions to inform the upcoming legislation.

From what I'm reading I bitterly opposed to this move toward Internet censorship by the heavy hand of an "Internet Czar".

Your proposal is full of threats and penalties for users, but I see no penalties/deadlines/responsibilities on the part of the government or the "Internet Czar" to avoid squelching free and legal speech.

Why are you creating a "Chinese firewall" to prevent Canadians from freely getting information from around the world.

Why are you determined to set up a "nanny state"???

This proposal reeks of a backroom "deal" between government and big Internet companies to put onerous obligations which will prevent new companies and even individuals to act as mediators or providers of content. And this will backfire! Once a fanatical party (OK, you damn Liberals are fairly fanatical on a number of issues I disagree with, but just imagine a future government far more fanatical) gets power I can easily see it blocking any attempt by the Liberal party to use servers or allow the public to create and serve commentary that is contrary to the new oligarchy's "prime directive" for "a fair and honest Internet", yes, one that only allows The Party in Power to dictate what Canadians can see and what Canadians and Canadian companies can put on the Internet.

This is utterly horrible. You people are idiots. You haven't consulted with real experts. You show no concern for the rights of Canadians or a recognition of a fundamental right in a free democracy for people to express and share their opinions!!!

I will fight you tooth-and-nail and work hard to create an army of anti-Trudeau, anti-Liberal party Canadians to punish you for this latest IDIOCY!!!

signed:

**Richard Yates** 

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act.

s.19(1)

# Felicia Mazzarello

From:	
Sent:	August 11, 2021 1:22 PM
To:	ICN / DCI (PCH)
Subject:	Re: The Government's proposed approach to address harmful content online
Follow Up Flag:	Follow up
Flag Status:	Completed
Categories:	РМ
Is it possible to receive a	receipt confirmation for my 10 August 21 email?
Thank you.	s.19(1)

Ted Reinhardt

s.19(1)

----- Original Message -----

From:

To: "pch icn-dci pch" <pch.icn-dci.pch@canada.ca>

Sent: Tuesday, August 10, 2021 9:01:56 PM

Subject: The Government's proposed approach to address harmful content online

# Felicia Mazzarello

From:	and the second second		
Sent:	August 7, 2021 10:24 PM		
To:	ICN / DCI (PCH)		
Subject:	Internet censorship	s.19(1)	
Follow Up Flag:	Follow up		
Flag Status:	Completed		
Categories:	Ale		

I am a Canadian citizen and many users do not want the government of Canada policing the internet. Russia and China have these policies, Canada should not. Censorship is a slippery slope.

This will force many Canadians to use VPNs on their devices which raises costs for Canadians to use internet.

Bart Janik

## Felicia Mazzarello

From: Sent: To: Subject: Kozinska, Julia <Julia.Kozinska@ombudsman.gc.ca> August 3, 2021 9:56 AM ICN / DCI (PCH) Have your say: The Government's proposed approach to address harmful content online

Hello,

The Office of the Federal Ombudsman for Victims of Crime (OFOVC) would like to submit on this consultation. Could you please let me know when the deadline is for a written submission?

Thank you,

Julia Kozinska

Team Leader, Policy and Complaints Review / Chef d'équipe, politique et révision des plaintes Office of the Federal Ombudsman for Victims of Crime / Bureau de l'Ombudsman fédéral des victimes d'actes criminels Government of Canada / Gouvernement du Canada julia.kozinska@ombudsman.gc.ca / Tel: 613-762-1574/ Fax: 613-941-3498

# Felicia Mazzarello

From: Sent: To: Subject: David Basskin -July 31, 2021 7:37 PM ICN / DCI (PCH) Paper on Harmful Content Online

Is the paper on this subject (on the web at <u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html</u>) available as a PDF document?

------

David A. Basskin David Basskin Consulting Inc.

s.19(1)

Cell: Email:

#### Felicia Mazzarello

From: Sent: To: Cc: Subject: Lusterio July 31, 2021 1:57 PM s.19(1) justin.trudeau@parl.gc.ca ICN / DCI (PCH) EmbraceHealthFoundation is your key ally in raising and advocating for an accountable Digital Citizenship for all! We need to be a big part of this change in legislation !

Dear Government of Canada/ Digital Citizen of Canada,

We are EmbraceHealthFoundation and one of the focuses of our self-esteem research and development focuses on the development of a more defined sense of morale ethical self.

This is one of our key indicators in our self-esteem assessment tool.We strive to bring accountability to self and others in all that we advocate for.

Our data and work history focuses on anti bullying and reducing harm for children and youth on line and is a huge part of our data base and now our resource base.

May we connect with the Heritage Minister or anyone who is most responsible ?And also the Innovation Minister working on data privacy regulations that flows laterally with all these insights.

We have key data and insights on the risks and harms of online risks."Online defamation, misinformation and disinformation is an ongoing health and social risk for children and youth and needs to be equated to

the most violent and aggressive acts in society," states Arlene Lusterio of EmbraceHealthFoundation.

We also have solutions based on our self-esteem research and development and our focus on innovation that can advance the solutions.

In the best descriptive capacity we have definitions, terms and data that need to be drafted into the legislation to support a safer digital world for Canadians .

We have a sincere interest in the drafting of this legislation in supporting the rights of children and youth and truly for everyone.to advance accountability.

EmbraceHealthFoundation and EmbraceHealthInnovations have been working for a long time in these spheres and have data and advocacy. policy and solutions to draft the best narratives for accountability and

the definition of an accountable Digital citizen. We also know too well how the system continually fails to be accountable. EmbraceHealthInnovations knows the tech sector and the big tech well as we are always on their

radar for being so disruptive and advocating for a more accountable digital world.Please reach out to us for more collaboration.Thank you for your time and consideration.

Regards, Arlene Lusterio EmbraceHealthFoundation.ca EmbraceHealthinnovations.ca

s.19(1)

From:	kellyja
To:	ICN / DCI (PCH)
Subject:	Proposed Internet Monitoring, Surveillance and Censorship
Date:	September 24, 2021 5:40:46 PM

I am writing as a Canadian veteran who lost many friends serving nine years in the Canadian Armed Forces as well as in NATO Germany as Canada's contingent.

I have almost family members in past great wars .

Let me simply day that I and ma y of my friends are ONE HUNDRED percent against the proposed censorship on the internet.

I find this egregious to myself, my fellow veterans and the fallen, to keep liberties, freedoms and democracy alive, for future generations.

Give people the credit they deserve intelligent beings capable of far more good than evil .

This in my experience, and especially in consideration of the current government policies is a deliberate act of malfeasance.

Please keep Canada a free, open and democratic country, where our constitutional rights mean something.

We are already living under near draconian government policies of driving and plotting Canadians against one another.

This is a deliberate act of further censorship depicts, very sick minds at work in government to further limit and control Canadians.

Stop the nonsense or otherwise veterans spirits will soon start haunting Ottawa and all politicians that think they are better, smarter or wiser than the average Canadian .

James Kelly

s.19(1)

From:	Alex Plevako (//E_ACCESS /O //
To:	ICN / DCI (PCH)
Subject:	Have your say: The Government's proposed approach to address harmful content online
Date:	September 24, 2021 5:59:22 PM

This is a waste of time and money.

The application and definitions are too broad.

The RCMP and CSIS (nor any other agency) should not be used to moderate or police these over-reaching new rules.

This is a hideous and awful idea. Stop it, forget it!

Focus your efforts to protecting consumer data privacy and security like Europe has done with GDPR as this is a much bigger, more pressing issue for ALL CANADIANS.

Thank you.

# Felicia Mazzarello

From: Sent: To: Subject: Martin French <martin.french@concordia.ca> July 29, 2021 6:39 PM ICN / DCI (PCH) PDFs of the Technical Paper and Discussion Guide?

Hi There,

Thanks for your attention to this email. Thank you for also leading this discussion on The Government's proposed approach to address harmful content online.

Do you have PDFs of the Discussion Guide and Technical Paper? I'm going to be working in a cabin (w/ no internet connection) over the next few days and I'd like to be able to read them.

Thanks,

Martin

Martin French - Pronouns he/him/his

Associate Professor, Sociology Department of Sociology and Anthropology

Interim Director Technoculture, Art and Games (TAG) Research Centre Milieux Institute for Arts, Culture and Technology

Concordia University, Sociology + Anthropology 1455 de Maisonneuve Blvd. W. (H-1125-17) Montréal, QC, H3G 1M8 Phone: 514.848.2424 x2110 Email: martin.french@concordia.ca Web: www.martinfrench.net www.risklogics.org @Martin\_A\_French

From:	Tracey Young	he Access to Information
To:	ICN / DCI (PCH)	
Subject:	Stop The Escalation of Censorship and Targeting of Canadians ar Canada	nd Their Charter Rights to Free Speech in
Date:	September 24, 2021 7:03:28 PM	

As a concerned citizen and taxpayer in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of advocacy, protest and personal expression.

This dangerous and tyrannical approach will increase censorship, intimidation, and silence the voices of women, racialized, and First Nations people who advocate for the civil and human rights of themselves, and their gender and racialized communities. This will also threaten the Fundamental Freedom of Expression, a key anti-oppression part of the Canadian Charter of Rights and Freedoms.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada. This ushers in a police state that has no place in a civil society or Parliamentary Democracy, such as Canada.

In Canada, the mainstream media -- largely managed and dominated by white, middle-aged privileged men, does not represent the diversity and voices of Canadians. This has become increasingly notable over the last few years with consolidation of media under large corporate media outlets. These corporations have demonstrably silenced women, racialized people, First Nations people, and other socio-cultural communities and pushed them and the important issues they advance further into the margins of society in Canada.

The tyrannical and oppressive voices of the "bought corporate media" in Canada have betrayed Canadians rights to have a diverse range of socio-economic, community, and social issues brought to the attention of wider audiences. Mainstream media does not serve the interests of a growing number of Canadians. This is why increasing censorship and silencing more diverse voices and the Charter rights of all Canadians to freely express themselves, and participate in online media, presenting their views and perspectives, as well as those of their communities must not be scaled up in Canada. This threatens the very fabric and integrity of Canada and further solidifies the institutionalization of colonialism in the 21st century -- something that should be a relic of the past.

These proposals are very likely to be used to police, intimidate, target, harass, silence, and criminalize already marginalized people on the Internet, not to protect and empower them to freely participate in their communities and society. Free speech must be protected, enhanced, and encouraged in Canadian society.

I urge you to work with civil and human rights advocates; academic experts; civil society; and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online. Canada already has public hate speech laws. However, what has become clear is that political and social elites in Canada feel entitled to use corporate media to attack, intimidate, silence, and threaten marginalized people with absolutely no consequences, or ramifications.

Over the last two years, we have many examples of this, such as the use of abusive, degrading, and pejorative language and targeting of Canadians with the use of terms such as "vaccine hesitant;" "anti-masker;" "anti-masker;" and "unvaccinated which are wielded by largely white, privileged elitist men to silence, and use dog whistle trigger words to intimidate and threaten the rights of Canadians to exercise free speech and Informed Consent over health care decisions, which is the law and jurisprudence in each Province and Canada. I have many examples of this and it

# Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

is my analysis that if these proposed changes come in that these elites -- some of whom include Premiers, Provincial Health Officers, and elected officials will be able to have complaints filed against them.

We already know that specific communities suffer higher rates of targeted oppression, harassment, persecution, and surveillance in Canada. There is no need for additional laws or policies -- especially those as draconian and dystopian as those being proposed to move forward in Canada. Our strength is in our diversity, inclusion, and opening up free speech.

Thank you for considering my thoughts and perspectives at this pivotal moment in Canadian history.

Sincerely,

Tracey Young

Marko Zatowkaniuk
ICN / DCI (PCH)
The harm of the currently proposed measures outweigh their putative benefits
September 24, 2021 7:45:05 PM

I strongly oppose the measures proposed in your consultation, including:

- mandatory 24-hour takedown windows where criminal activity has not been established by courts;
- forcing platforms to proactively surveil their users' posts for non-criminal activity;
- and any plans for blocking of websites in Canada where criminal activity has not been determined by courts.

The measures proposed will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

For online platforms, it is easier to over-censor than to carefully weigh and evaluate each and every post in a nuanced manner. This is what they will do.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Marko Zatowkaniuk

 From:
 james elliott

 To:
 ICN / DCI (PCH)

 Subject:
 harmful content proposal

 Date:
 September 23, 2021 10:08:19 AM

What the hell guys? This is terrible. Do you not see the massive potential for abuse?

You need to either let someone who knows what they're doing write internet laws or you need to just step out of the game. Shame on you.

-James Elliott

s.19(1)

 From:
 ICN / DCI (PCH)

 Subject:
 Digital Citizen Initiative: my response

 Date:
 September 22, 2021 10:46:51 PM

Having read the discussion guide provided, I want to give my feedback regarding the proposed Internet regulation reforms.

I am a contributing writer to a website that is a major Canadian info centre for likeminded individuals to read and discuss our particular alternative philosophy. Unfortunately, people of our worldview have a tendency to be burdened with accusations of "hate speech". The concern I have is being targetted for deplatforming by this new regulation, even though I write in a respectful manner and have never called for violence.

I am also concerned that the new Internet regulatory framework would have a less than ideal cost-to-effectiveness ratio. I do not believe that service providers based outside of Canada can be effectively bridled by a new or evolved federal agency here.

Thanks for reading.

Jordan C Lewans

Sent with

the secure & ad-free mailbox.

From:	Luiz Gonzaga dos Santos Filho MCCE.	S
To:	ICN / DCI (PCH)	
Subject:	I say no to the Government's proposed approach to address harmful content onlin	ne
Date:	September 22, 2021 7:10:07 PM	

In regarding to: https://www.canada.ca/en/canadian-heritage/campaigns/harmful-onlinecontent.html

I express my vehement disapproval of it. My arguments are summarized here https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filtering-blocking-and-reporting-rules-1

That's the opposite of the inclusive culture we like about Canada!

From:	Katy Churchill
To:	ICN / DCI (PCH)
Subject:	Digital Citizen Initiative Feedback
Date:	September 22, 2021 5:56:45 PM

Hello,

s.19(1)

and a Canadian citizen, I have several concerns about the new legislative and regulatory framework as proposed. The laws already existing in Canada give plenty of power to law enforcement already to go after CSAM and non-consensual images, the issue seems not to be a lack of laws but rather a lack of interest or funding to enforce the existing laws.

I am referring to all forms of sex work that are legal in Canada, including porn videos and webcam performing) with many social media platforms banning their accounts simply for being in the sex industry and not for breaking terms of service. In concert with the latest moves from the financial industry, putting the new rules in place as proposed will have a huge impact

The current

moral panic in the media has been driven by Christian evangelical organizations who conflate consensual sex work with trafficking and child abuse, and it is simply not true.

Please do not allow government policy to be dictated by American special interest groups who have a stated goal of making all pornography illegal. Or, if you do wish to outlaw porn, be honest about it and don't hide behind "think of the children" or "but it's all trafficking". Parents are responsible for their children, not politicians.

Yours truly, Katy Churchill

From:	Sierra Angus
To:	ICN / DCI (PCH)
Subject:	Proposed approach to address harmful content online
Date:	August 11, 2021 6:02:12 PM

#### Hi there,

Personally the way that the government plans to leave such an open ended evaluation of 'harmful content' with such little time for diagnosis and evaluation of it appears to be a gross overstep of personal boundaries and speech. Its frankly unconstitutional and is not just terrible to read but also remarked as one of the worst approaches in the world which is embarassing for the cabandian government at best and an abuse of its citizens rights at worse.

The proposal for actual regulation also sets up only the biggest of tech giants (who are already know to have much too large of a control of the spread of harmful speech and an abuse of their funding and influence) to be suztainable in the long run, destroying any accessibility for any other competitor to join the market space. Quite Frankly it would suck for anyone who isnt deeply deeply enamored with these massive horrible corporations which isnt a lot of people.

This proposal is awful and a sham and should be thrown away. Not even a revision could improve it at this point. There are ways to properly attempt to detect and monitor harmful speech that doesbt also violate the citizens of the country. Once again, embarassing to read that this was even proposed as it would be soley used for political gain and essentiallyminority targeting.

Actually wishing the worst regards on yall!

From:	Shane Phillips
To:	ICN / DCI (PCH)
Subject:	Bill C-36
Date:	September 22, 2021 3:20:24 PM

- "Online Criminal Content Regulation" is a more accurate nomenclature until the proposal addresses other harmful content that doesn't rise to the level of the criminal definitions. "Beverage regulation" would not be an accurate name for a bill that only addressed alcoholic beverages.
- Consult and re-scope the definitions of harmful content. In particular, examine the impact of adopting narrow definitions from the *Criminal Code* and related case law versus broader definitions in terms of the reality of content moderation practices and harmful content sought to be reduced. The approach should be clear and justification provided.
- In evaluating harmful content, ensure that situations are captured where volume and persistence creates a situation of harm, even where any individual act or post would not violate the regulations.
- Introduce laddered obligations drawing from the *Digital Services Act*. There should be specific and more onerous obligations on major platforms, however defined, but other platforms should not be entirely out of scope.
- Consultation on the details of the proposed Digital Rights Commission with a focus on how to structure it to balance rights and ensure access to justice.
- The proposal of a general obligation to monitor all harmful content should be categorically rejected. Consultation should be undertaken to explore options that are proportionate and effective to achieve the objective of reducing circulation of harmful content
- The 24-hour time limit should be abandoned in favour of a generic obligation to act expeditiously. Or, at minimum, exceptions should be drafted, which allow additional time to engage in a contextual analysis of expression in the grey zone, similar to the NetzDG model.
- Incentivize platforms to protect free expression when making moderation decisions in order to avoid blanket removals. Consider addressing the prevalence of harmful content, not merely its presence.
- Explore more creative options. For example, the Digital Services Act incorporates a
   "trusted flagger" system wherein complaints from a verified trusted flagger (person or
   organization) can be handled on an expedited basis. The status of the trusted flagger is
   contingent on the accuracy and quality of complaints made. If a trusted flagger has a
   certain number of "false positives" they can lose their status.
- Maintain tightly limited scope and availability of this enforcement measure (24 hour removal), including requiring judicial authorization.
- Add warning steps and procedural protections to ensure platforms can make representations before drastic measures are pursued.
- Examine limiting website blocking to specific web pages, or when that is not possible, to OCS that are primarily devoted to sharing illegal content.
- Limit mandatory reporting to circumstances where it is reasonably suspected there is an imminent risk of serious harm.
- Limit the basis for mandatory reporting, to a complaints-based approach or reasonable awareness.
- · Do not impose proactive monitoring coupled with any mandatory reporting.
- · Platforms should still be required to address systemic problems, but the proposal should

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

avoid framing the requirement as a "gotcha" on platforms, rather enlisting Platforms as n Act collaborators, and using data from transparency reports as an accountability tool.

 Consult with platforms and organizations such as GIFCT and the Global Network Initiative about appropriate and achievable transparency reporting requirements.

Shane Phillips

 From:
 John Brooks

 To:
 ICN / DCI (PCH)

 Subject:
 Abandon this harmful proposal

 Date:
 September 22, 2021 3:06:51 PM

s.19(1)

I am a Canadian Citizen I want to voice my vehement disagreement with your proposal to "address harmful content online". This is massively overreaching the role of the government. You are creating a public-private partnership with the purpose of circumventing Canadians' Charter Rights, under the guise of protecting vulnerable groups, and making targets out of Canadians for anything that an opaque, proprietary system flags as potentially harmful, creating an unhealthy and invasive surveillance regime.

This is absolutely appalling and unacceptable.

- John Brooks

From:	Jackyn W (NE ADDESS /
To:	ICN / DCI (PCH)
Subject:	Comments on the Government's proposed approach to address harmful content online
Date:	September 22, 2021 10:38:12 AM

Good morning,

I am sending brief comments regarding the proposed approach to address harmful content online.

While the intent of this policy is good, I believe that it is not the governments place to be censoring what they consider as hate speech from the internet. Due the relative nature of hate speech (changes depending on religion, race, etc.) there is no way to define it such that one group is happy and the other is not.

I do agree with the government taking better action against child pornography. Frankly, that should not even exist, and it is sad that Canadians can access it so easily.

Thank you, Jaclyn

 From:
 Sandra Harrison

 To:
 ICN / DCI (PCH)

 Subject:
 Public Consultation regarding online harms

 Date:
 September 17, 2021 12:54:01 PM

This is in response to a request for public consultation on online harms. I would like to comment on 2 of those harms: CSAM and the non-consensual sharing of intimate images.

## I would like you to focus on the following priorities:

- Ensure that sites who frequently host CSAM and/or intimate images shared without
  consent do not receive criminal immunity from past offences and will be held criminally
  responsible if they do not comply with the regulatory demand
- Sites must be required to take robust proactive measures to prevent uploading CSAM and/or intimate images shared without consent, including verifying the age & consent of all those depicted prior to hosting content
- Adopt the proposed changes to strengthen the Mandatory Reporting Act

In regard to the options about which information sites would be required to give to law enforcement when they report CSAM, please adopt option #2, which would be user's basic subscriber information. I prefer this option as it would allow law enforcement to locate offenders and rescue victimized children faster.

I look forward to hearing you have taken these steps to help those suffering from sexual exploitation.

Sincerely,

Sandra Harrison

From:	Plerre Beauregard (NELACCESS (C
To:	ICN / DCI (PCH)
Subject:	Online Harms consultation- Digital Citizen Initiative - Department of Canadian Heritage
Date:	September 17, 2021 10:48:42 AM

To whom it may concern,

As a private citizen who has been involved in advocacy for the promotion of age verification online, I would like to ask that the minister responsible would insure the new regulatory framework which would oversee Online Harms, prepare to support the age verification bill which had been approved in the Senate in june 2021 and was ready to begin it's process in the house of commons. That bill was initiated by Senator Julie Miville-Dechêne and is titled An Act to restrict young persons' online access to sexually explicit material Bill S-203. See details here

I would also request that the regulatory framework:

- Ensure that sites who frequently host CSAM and/or intimate images shared without consent do not receive criminal immunity from past offenses and will be held criminally responsible if they do not comply with the regulatory demands
- Require sites to take robust proactive measures to prevent uploading CSAM and/or intimate images shared without consent, including verifying the age & consent of all those depicted prior to hosting content
- Adopt the proposed changes to strengthen the Mandatory Reporting Act. 2 options have been outlined of what information sites would be required to give to law enforcement when they report CSAM. I would ask that the regulatory framework to adopt option #2, which would be user's basic subscriber information. This would allow law enforcement to locate offenders and rescue victimized children faster.
- Follow recommendations of the Ethics Committee (THIRD REPORT -Pursuant to its mandate under Standing Order 108(3)(h), the committee has studied the Protection of Privacy and Reputation on Platforms such as Pornhub and has agreed to report the following:... click here for full report.) . A special attention should be given to recommendation number 2 copied below.

Recommendation 2 concerning the duty to verify age and consent

That the Government of Canada mandate that content-hosting platforms operating in Canada require affirmation from all persons depicted in pornographic content, before it can be uploaded, that they are 18 years old or older and that they consent to its distribution, and that it consult with the Privacy Commissioner of Canada with respect to the implementation of such obligation.

Pierre Beauregard

s.19(1)

#### Hi There,

Here's what I think: Defending groups from words will likely end up oppressing the individual. You have proposed serious penalties for "wrong think". We all think we know what you mean when you say hate, but this is going to be used to turn awkward, curt, unwoke criticism into hate speech. I appreciate the very Canadian idea of not being offensive but this is worded in such a way as to make ordinary ideas punishable.

For example, under this law, and we must try to imagine this sprawling out over time, will a Canadian be able to

- Question their minor child's self-diagnosis of gender dysphoria? Will they be able to talk about the risks of this decision publicly without being punished?
- Will I be able to blasphemy? Can I say god doesn't exist? If I am an atheist will it be ok to say God does exist? Can I say religion is a man-made silly charade to control people? Can I say that publicly?

Additionally, anytime you are flagged by the police, or otherwise find yourself in the "system" you are at risk: risk of unjust prosecution, wrongful arrest, reputation destruction, anxiety and ostracization. This law makes it easier for people who utter words to end up in the "system". This puts them at risk, especially marginalized people. I am against making it easier to be reported to the police.

This will end in many individual tragedies even if some groups can claim pyrrhic victories. So my final point:

Where, in this law, can one find redress from the harms this will inevitably cause to innocent individual Canadians for whom this law is used to persecute?

Or do we think groups are more important than individual Canadians?

I vote no on this bill as it stands.

Thank you Stephen LeMieux

From:	Stephan Borau the Abcess to Inform	
To:	ICN / DCI (PCH)	
Subject:	Digital Citizen Initiative The Government's proposed approach to address harmful content online	
Date:	September 16, 2021 8:51:26 PM	

Good day.

I have a few concerns regarding the proposed approach to address harmful content online:

- "Terrorist content" as a category is rather vague. The previous Harper Government was beginning to call environmental activists – "terrorist groups". This legislation needs to carefully consider how current or future gov'ts might interpret this proposed legislation;
- "Hate speech" also needs to be carefully defined in regards to the proposed regulatory approach as opposed to a criminal approach;
- Judicial authorization should still be required to obtain transmission data or BSI (there continues to need to be checks-and-balances on the police -- they should follow due process).

Overall, this process of asking Canadians to "Have your say" is not robust or userfriendly. Somehow I was alerted to this page, but there is no systematic process in place to gather this input from the citizens of this country. It comes across as a typical government consultation process, half-hearted at best.

Have a good day.

Stephan A Borau s.19(1)

From:	Linda Audette
To:	ICN / DCI (PCH)
Subject:	hate speech by the government?
Date:	September 13, 2021 8:56:21 AM
Dute.	September 13, 2021 0.30.21 AF

To whom it May Concern

I found this on the web I am all for stopping hate speech!

I recently has hate speech and what appeared to be threats by our own Prime Minister of Canada

That protestors "should be condemmend" "and corrected"

Now I was not swearing or threatening! I was trying to reach the Prime Minister with my message and concerns for my community, that I feel my voice is not being heard, and that doctors and nurses and scientific evidence is being manipulated and blocked by our government and main stream media.....these are facts. How will the Federal government decided what is "Online Harms" when the head of our government or a political party not follow their own suggested legislation? This is very concerning to me as I feel I do not have a voice

Thank you for your time s.19(1) Concern

# Canadian government's "Online Harms" legislation

Posted on July 31, 2021 by admin

The Canadian federal government sent an <u>email</u> this week to civil liberties associations and other groups announcing the opening of the government's consultation period on its proposed "Online Harms Legislation". The email included slides in an <u>attachment</u> with information about the legislation, entitled "Technical Discussion Paper: Online Harms Legislation". The legislation will regulate social media expression that the government deems to be "hateful" or "harmful".

The slides state "there is a clear role for Government" in regulating online speech and that "efforts by social media platforms are inconsistent and not enough". The government proposes to "set new rules for social media platforms", including:

Obligation to remove 5 categories of harmful content (hate speech, child sexual exploitation content, non-consensual sharing of intimate images, incitement to violence content, and terrorist content) Harmful content to removed within 24 hours of being flagged Transparency, reporting and preservation requirements Procedural fairness for users, victims, and advocacy groups Direct internet service providers (ISPs) to block access in Canada as a last resort with a court order, for platforms that persistently do not comply with orders to take down child exploitation and terrorist content

The legislation would also create a new Digital Safety Commission to "oversee and enforce new rules", "make binding decisions on content removal", and "provide independent recourse through a digital tribunal system".

The forthcoming legislation may also:

Require social media platforms to inform the Canadian Security Intelligence Service (CSIS) about certain types of information posted on their platforms (slide 10).

Provide CSIS with a new judicial authorization for obtaining consumers' internet subscriber information such as the transmission data, customer name, address, phone number, billing information associated with IP address (slide 12).

The consultation period ends on September 25, 2021. Comments can be submitted to the government at: pch.icn-dci.pch@canada.ca.

Sent from Mail for Windows

From:	Chauncey McAskill
To:	ICN / DCI (PCH)
Cc:	David.Lametti@parl.gc.ca
Subject:	Comments on Bill C-36
Date:	September 12, 2021 10:24:24 AM

Hello,

The government has patched together some of the worst ideas from around the world:

• 24 hour takedown requirements that will afford little in the way of due process and will lead to over-broad content removals on even questionable claims;

 website blocking of Internet platforms that won't abide by its content takedown requirements;

· a regulatory super-structure with massive penalties and inspection powers;

· hearings that may take place in secret in some instances; and,

 regulatory charges that may result in less choice for consumers as services block the Canadian market.

Meanwhile, core principles such as the Charter of Rights and Freedoms or net neutrality do not receive a single mention.

Given the framing of the documents, the short window for comments, and the little attention from the media, it is clear that this is little more than a notification of the regulatory plans, not a genuine effort to craft solutions based on public feedback.

For a government that was elected with a strong grounding in consultation and freedom of expression, the reversal in approach could hardly be more obvious.

Regarding 24 hour notice and takedown, the government should, at the very least, follow the NetzDG in Germany and provide 7 days to more carefully assess the content. Coupled with the administrative and monetary penalties for non-compliance, OSCs systematically err on the side of taking down lawful content in order to avoid risk to themselves.

Under current systems in both Canada, USA, and elsewhere, take downs are already a powerful tool wielded by various parties (both individual, masses of individuals, and corporations) to censor lawful content that does align with their interests.

The proposed legislation requires proactive monitoring which is exactly the kind of filtering mandate that has had civil society and human rights advocates ringing alarm bells in Europe for several years. A much narrower proposal in the EU Terrorist Content Reg drew condemnation from <u>UN human rights officials</u> and more.

The proposed legislation requires OSCs to report users who might have violated the law to police. This kind of privatized dragnet surveillance of user speech is in Germany's new NetzDG law too. Google is <u>challenging</u> it there.

I may not be an expert in law, but I do live in the world. So I think I can spot an issue about who gets reported to the police, and how police treat them. We have every reason to expect people of color and other marginalized or vulnerable groups to get flagged more, reported to police more, and mistreated more after that happens. The problem can start with <u>bias in AI</u> or

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

The harms from platforms surveilling users and reporting them to police will also disproportionately hurt vulnerable groups like undocumented immigrants, parolees, or sex workers — whether by getting them silenced, banned, and reported, or by causing self-censorship.

The US has been coming to <u>terms</u> with this problem in its last platform law, SESTA/FOSTA - to the point that Elizabeth Warren and other Members of Congress have called for a <u>formal</u> assessment of harms to sex workers.

The new regulatory bodies are being given sweeping powers to hold over online speech.

Regarding the legislation against Canadian ISPs, this reminds me of what the USA tried to do —in SOPA/PIPA—of which multiple UN and regional human rights officials wrote to <u>object</u>. In other parts of the world, law has been shifting to tolerate site-blocking in extreme cases, like where an entire site is dedicated to counterfeiting or piracy. But this seems to be about blocking entire sites that have lots of legal speech, and just some that's illegal.

Respectfully, Chauncey McAskill

From:	Ariana Magliocco
To:	ICN / DCI (PCH)
Subject:	[Comments] Harmful Online Content
Date:	September 11, 2021 3:38:31 PM

Dear Digital Citizen Initiate,

I am emailing to express my concerns about the proposed draft legislative and regulatory framework for harmful online content. While I understand and applaud the intended purpose of this legislation, there are a few key issues I have been able to identify which I believe require greater attention.

- Proactive monitoring and filtering: I am deeply concerned that by deploying automated tools to police online information, we will see a rise in new-reporting, education and counter speech being flagged, taken down or censored. We have already seen the failures of AI technology on platforms such as Facebook or Instagram to incorrectly flag and take down social justice content (such as BLM posts, etc.) There is reason to be concerned that marginalized voices will only be further marginalized on online spaces.
- 2. Platform reporting to law enforcement: I am concerned that, as mentioned previously, that inherent biases will contribute to the disproportionate policing of marginalized peoples. I believe there is good reason to believe that this provision will target vulnerable groups such as undocumented immigrants, parolees, or sex workers.

Ultimately, I am deeply concerned that this legislation will lawmakers develop legal definitions of "harmful" speech beyond what has already been set out in Canadian law. Without a diversity of voices which center folks lived experiences, I worry that the ramifications of this will impact already marginalized peoples.

I look forward to hearing how these issues will be addressed as this legislation moves forward.

Best,

Ariana Magliocco

Jason Montgomery (DE A
ICN / DCI (PCH)
Re: Government"s proposed approach to address harmful content online
September 10, 2021 11:19:55 PM

While child porn, terrorist content, and hate speech online are very real problems, the Government of Canada's current proposals go too far. Filtering systems can be gamed and produce false positives, blocking non-complying websites like in China, short deadlines, and invasive data retention policies threaten all Canadians' rights to freedom of speech and privacy.

This article from author Cory Doctorow summarizes my feelings: https://doctorow.medium.com/canadas-got-the-world-s-worst-internet-ideas-e1ae6124db2a

Thank you,

s.19(1)

Jason Montgomery

From:	Jake Ku	
To:	ICN / DCI (PCH)	- 10(4)
Cc:		s.19(1)
Subject:	Comments on new framework	
Date:	September 9, 2021 6:13:04 PM	

I am horrified to see that the government's proposals are a hodge podge of rejected and failed ideas. Many of the tactics proposed have been challenged and defeated by various Rights advocacy groups around the globe. This is not the sort of stuff we ought to be recycling.

I am opposed to the government dictating what Canadians citizens may or may not post, write, see or read online. The type of filtrering you propose illustrates that you have no real clue how the technology used to implement these filters works. What is proposed in the framework will not work the way they say it will, and is very likely to create more problems while solving none.

The framework lays out a set of regulatory powers so vaguely worded as to make them legally omnipotent. I am completely opposed to any framework that grants broad unambiguous power to ANY governing body, let alone one that doesn't even exist yet and may not be necessary at all. Also deeply troubling is the absence of any plan or measure to protects Freedom of expression or any of the other rights set out in our Charter.

What the framework proposes is the constant filtering/monitoring of citizens online activities AND the automatic reporting of suspect activities to law enforcement. This is the sort of Orwellian nightmare that, as a Canadian, I thought I was safe from. Is that really the world you want to live in? Do you want a criminal record for sending a risque photo? Do you want the government to know constantly and at all time precisely where on the internet you like to go? Do you trust that all that data will be safe and never abused? Do you you want to surf over to your favourite blog/podcast/content creator only to find that the government has used ISP blocking to digitally blacklist them? I certainly do not.

The framework is not only offensive to me as a freedom loving Canadian, it proposes such technically absurd solutions (to problems which are of a questionable relevance) that it will almost assuredly create more problems and solve next to none.

TL:DR - The proposals outlined in this framework will make living in Canada worse, not better. I will oppose them at every step.

Thank you for your time, Good Day

Jake Ku

 From:
 Nancy Brown

 To:
 ICN / DCI (PCH)

 Subject:
 Social Media Platforms

 Date:
 September 9, 2021 4:40:12 PM

 Attachments:
 BRIEF.docx

Please find enclosed my comments for government consideration with regard to rules for how social media platforms and other online services must address harmful content. Thank you, Nancy Brown

Sent from Mail for Windows

To: Digital Citizen Initiative

Department of Canadian Heritage

25 Eddy Street

Gatineau, Quebec, K1A 0S5

From: Nancy Brown,

Lailia Mickelwait, Founder and CEO of Justice Defense Fund reports that the German government is set to shut down Pornhub in the country along with three other major porn tube sites, YouPorn, MyDirtyHobby (both owned by Mindgeek), and XHamster for their failure to implement mandated child protection procedures. This move will block the non-compliant porn sites from 83 million people for their ongoing abuse of underage victims both in front of and behind the screen.<sup>3</sup>

s.19(1)

If Germany can do it, why not Canada? This is an amazing turn of direction for Germany. Many critics say that Germany's liberal approach with its sex laws has spectacularly failed, normalizing prostitution and turning the country into what they now call the 'bordello of Europe'.<sup>2</sup> With their laws, the number of prostituted person has grown to over 400,000 victims, mostly women and girls. These victims of sex trafficking are most likely to originate from Romania, Bulgaria, Nigeria meaning that traffickers tend to target immigrants, due to the fact that immigrants in Germany are far more likely to live in poverty than German citizens.<sup>3</sup>

In addition, Germany is considered a country of destination for cross-border trafficking in children for sexual purposes, and it is also a producer of pornographic materials. Cities such as Berlin, Hamburg, Frankfurt, and Mannheim are destinations for trafficked children.<sup>4</sup>

The intersection of sex trafficking, prostitution and pornography are a given as pornography is a pipeline for prostitution and sex trafficking. One does not exist without the other in most countries.

Germany's effort towards a cultural and behavioral change is a remarkable and commendable shift which Canada ought to follow. Canada is in a position to be a leader in this movement, demonstrating accountability and responsibility to the world by shutting down Pornhub which is located in Montreal, Quebec. Why is our government so complicit in continuing this oppresive suffering of women and children when our government claims to support gender equality?

<sup>&</sup>lt;sup>1</sup> Pornhub and XHamster set to be banned as country brings in strict child protection laws. Rory Ellis, 28 July 2021 www.dailystar.co.uk

<sup>&</sup>lt;sup>2</sup> Mega-brothels: Has Germany become 'bordello of Europe?' Jim Reed. BBC News. 21Feb.,2014

<sup>&</sup>lt;sup>3</sup> 5 Facts about Human Trafficking in Germany. Leo Ratte. The Borgen Project <u>http://borgenproject.org/human-trafficking-in=germany</u>.

<sup>&</sup>lt;sup>4</sup> Sex Trafficking of Children in Germany. Stop Sex Trafficking of Children and Young People. <u>www.ecpat.org/wp-</u> <u>content/uploads/2016/04/Factsheet\_Germany.pdf</u>

Reflecting on your committee's recommendations and list of participants, there appears to be a strong bias, many omissions and a central focus of male dominated industries and techology conglomerates with little or no reference to the voices of survivors or women's organizations that are struggling to support the victims of techological abuse and violence. This is a bilantant illustration of an imbalance of power, both financial and gender with possible racial biases.

In the USA, a group of survivor-focused law firms have filed a class action lawsuit against MindGeek, the parent company of Pornhub. Listen to the stories of two women whose lives were permanently harmed by the action of MindGeek. These are just two stores that could be multiplied by many similar Canadian stories.

"Plaintiff Jane Doe#1 was just 16 years old when she was drugged and raped by a man in Tuscaloosa, Alabama. The child sexual abuse and rape of Jane Doe #1 was filmed. That same man entered into an agreement with MindGeek to share profits from views and downloads of Jane Doe #1's victimization on MindGeek's websites. MindGeek reviewed, categorized, tagged and disseminated the images and videos depicting the rape and sexual exploitation of sixteen-year-old Jane Doe #1. One of the videos of Jane Doe #1 had been viewed over 2,400 times since MindGeek added it to its website in early 2018.

At no time did MindGeek or Pornhub attempt to verify Jane Doe's #1's identity, age, inquire about her status as a victim of trafficking or otherwise protect or warn against her traffickers before or while the video of her being drugged and raped was sold, downloaded, viewed and otherwise advertised on Pornhub.

Plaintiff Jane Doe #2 was still a minor when a sex trafficker forced Jane Doe #2 to participate in the creation of sexually explicit videos that included adults engaging in sex acts with her. Videos of adults engaging in sex acts with Jane Doe #2 when she was a minor were uploaded and disseminated through websites owned, operated and/or controlled by MindGeek including Pornhub. Neither Pornhub, not any other website, owned or operated by MindGeek undertook any meansure to verify Jane Doe #2's identity or age. As a result, child sex abuse material depicting Jane Doe #2 was distribute broadly throughout the world on MindGeek's internet platforms.

The plaintiffs are suing MindGeek for financially benefiting from their abuse, which violates the Trafficking Victims Protection Reauthorization Act, among other laws.<sup>5</sup>

Imagine the damage done to these persons as well as all the thousand other Jane Doe's throughout Canada who have been permanently harmed for life. eChildhood published a report in 2020 called, A **Public Health response for the Safety and Welling of Children and Young People**. Numerous research projects have substantiated the multiple harms done to children. eChildhood has published a **Research Update** to highlight five major areas of harm, a definite link between the potential negative impacts and children and young people's access to pornography. These five major areas are as follows:

• "Shaping sexual attitudes and behaviours – such as earlier sexual experimentation, casual sexual behaviour and more 'risky' sexual behaviour;

<sup>&</sup>lt;sup>5</sup> Statement – Class Action Lawsuit Filed Against Pornhub by 2 Survivors of Childhood Sex Trafficking. NCOSE Statement. www.endsexualexploitation.org/articles.

 Poor mental health – including, but not limited to, being distressed and upset by the images, self-obectification and body image concerns, sexual conditioning, and developing compulsive sexual behavior disorders;

- Sexism and objectification such as reinforcing gender roles that women are 'sex objects', and men should be dominant while women should be submissive;
- Sexual aggression and violence consistently, there is a demonstrated association between regular viewing of online pronography and the perpetration of sexual harassment, sexual coercion and sexual abuse by boys;
- Child-on-child sexual abuse an under-researched area, professionals are noting an increase of this behaviour, influenced by children's access to pornography."<sup>6</sup>

The evidence of harm speaks for itself and can not be ignored in any way while considering legislation for restrictions of online access and viewing.

Our Canadian government has the responsibility to curb, curtail, or end freedoms that enfringe or cause harms to others. As Isaiah Berlin so clearly states "the extent of a man's or a people's liberty to choose to live as he or they desire must be weighed against the claims of many other values, of which equality or justice or happiness or security or public order are perhaps the most obvious examples. For this reason, it cannot be unlimited." Berlin goes on to say "total liberty for wolves is death to the lambs"<sup>7</sup>

Thus the actions of MindGeek must be curtailed and shut down to protect the lives of innocent children in Canada.

The Canadian Centre for Child Protection has done extensive research, one called, **Reviewing Child Sexual Abuse Material** reporting functions on Popular Platforms, in which they discovered, "Millions of images of child sexual abuse circulate freely on the internet each day, not only in obscure corners of the dark web, but also on some of the most popular web platforms. The Canadian Centre for Child Protection's (C3P) research found most web platforms lack content reporting functions specific to child sexual abuse material (CSAM). In contrast, with copyright infringement, reporting tools devoted to the issue are largely a universal standard. Our surveys with survivors — many of whom attempt to selfmonitor the spread of their abuse imagery — often cite ambiguous reporting functions as a factor in their ongoing re-victimization. By failing to adopt CSAM specific reporting tools, these companies inhibit their ability to take swift action in prioritizing and removing this illegal content. This state of content reporting is generally inconsistent with the goals of the **Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse,** established by the Five Country Ministerial, and adopted by some of the largest technology companies. C3P provides five key recommendations technology companies can adopt to immediately reduce harm to children and survivors.<sup>8</sup>

A UN report called **Cyber Violence Against Women and Girls: A Wake Up Call**, reports that the "The sheer volume of cyber–Violence Against Women and Girls (VAWG) has severe social and economic

<sup>&</sup>lt;sup>6</sup> eChildhood 2020 Update: Statement of Research Relating to Pornography Harms to Children. Prepared by Walker, L. & Kunaharan, S. https://www.echildhood.org/statement

<sup>&</sup>lt;sup>7</sup> Berlin, I. (1998(b). "Two concepts of liberty," in the proper study of mankind: An Anthology of Essays. New York: Farrar, Straus, and Giroux, page 240

<sup>&</sup>lt;sup>8</sup> Canadian Centre for Child Protection. Reviewing Child Sexual Abuse Material Reporting Functions on Popular Platforms. www.protectchildren.ca

implications for women and girls. Threats of rape, death, and stalking put a premium on emotional bandwidth and put a stress on financial resources, (in terms of legal fees, online protection services, and missed wages, among others). The direct and indirect costs to societies and economies are also significant, as needs for health care, judicial and social services rise, and productivity goes down with the sense of peace and security required for business to thrive. Cyber VAWG can also have adverse impact on the exercise of and advocacy for free speech and other human rights."<sup>9</sup>

Thus, many Canadians agree that pornography is a serious public health issue in Canada as it is addictive, accessible, anonymous, and affordable. Defend Dignity has articulated "four specific ways pornography harms mostly children and women (men and LGBTQ+ individuals can have similar experiences) who have a lived experience of sexual exploitation and/or trafficking for sexual purposes.

1.) Pornhub is complicit in the grooming of exploited and trafficked victims.

2.) Pornhub is complicit in teaching children racism, misogyny, sexual violence, and normalization of pedophilia

3.) Pornhub is complicit in the trafficking of women.

4.) Pornhub is complicit in the publication and sharing of child sexual abuse material and nonconsensual images.

Data gathered from the intake forms of survivors Defend Dignity has served, provides the framework for our focus and the recommendations we make to the Committee.<sup>10</sup>

It is urgent that your committee moves and adapts the recommendations put forward by the ethics committee ......

This is not an issue that can wait – government needs to move to action immediately. I plead that you listen to the voices of numerous young women and girls whose lives have been forever destroyed by the neglect of government to legislate necessary limits on the technology industry primarily run by male wealthy leaders. In a recent report entitled "Increase in child pornography reports in BC" by Kendra Mangione in CTV NewsVancouver.ca "According to Stat Can, the rate of police-reported child pornography was up 23% last year. There are 2,178 more incidents reported in Canada in 2020 than in the year before, with the majority of incidents in Quebec and BC. In all of Canada last year, there were 7,200 cybercrime-related child pornography violations, up 34% from 5, 375 in 2019."<sup>11</sup>

If Canada has any sense of integrity and concern for the future of our young people, it must move quickly on legislation that would require age verification on all sites with adult content. Please follow the recommendation as outlined by the Ethics committee.

As the rest of the developed world is waking up to this social crisis of child porn exposure, I plead with our Canadian Government to show some much-needed urgent leadership to shut down Pornhub and to ensure age verification al all sites with adult content.

<sup>&</sup>lt;sup>9</sup> Cyber Violence Against Women and Girls: A Wake-Up Call UN <u>www.broadbandcommission.org</u>

<sup>&</sup>lt;sup>10</sup> Submission to the Standing Committee on Access to Information, Privacy and Ethics. Defend Dignity. February 2021

<sup>&</sup>lt;sup>11</sup> CTVNews Vancouver.ca "Increase in child pornography reports in BC. Kendra Mangione.

Listen to the voices of the following:

"Individuals who have been victimized are faced with the overwhelming task of trying to remove illegal content that should never have been distributed and profited from in the first place. It's time for pornography websites to be held accountable. Content should not be hosted without proof that all the individuals depicted are adults and have consented to both the creation and distribution of the material on that platform." **Defend Dignity** 

#### "It is unacceptable that companies such as MindGeek have operated with impunity while profiting off traumatic experiences of sexual assault, exploitation, and sex trafficking. Canadians must take a stand and insist that our country not be a safe haven for people to financially benefit from the recorded sexual victimization of anyone - especially youth. The SISE Act is a necessary step in ensuring that those who capitalize on filmed sex crimes are held accountable for the immense harm their actions cause."

Andrea Heinz, Activist, Exited from the Commercial Sex Trade in Edmonton, Alberta

"We know that companies like Pornhub have facilitated and distributed the uploading of videos of minors being sexually exploited and assaulted. We also know that non-consenting adults and trafficked women have been raped and tortured for the world to see. It is the role of Parliament to protect its citizens from predatory industries and the SISE Act provides important tools to help accomplish this."

#### Megan Walker, Executive Director, London Abused Women's Centre

The National Council of Women of Canada (NCWC) welcomes the proposed Bill "Stopping Internet Sexual Exploitation Act" that calls for amendments to the Criminal Code to protect those whose rights are brutally ignored. Content, acquired and shared without consent, is unacceptable in a just society. That children, who cannot "give" consent, are victims is to contravene all principles and laws, including the Convention on the Rights of the Child. The distribution of adult content must include a verification process that establishes that all participants are of legal age and that all participants depicted have consented to the distribution and commodification of the material. That material acquired and commodified without consent continues to circulate is to revictimize the victims. Pornography websites and other platforms must be held accountable."

#### Patricia Leson, President, National Council of Women of Canada

The Salvation Army has worked closely over the years with people who have experienced or survived sexual exploitation. We know that their voices and wishes are rarely heard or respected. The Stopping Internet Sexual Exploitation Act is an important step toward establishing safeguards to protect adults and minors from having unwanted images of them posted and shared over the internet for commercial gain at their expense." Commissioner Floyd Tidd, National Leader, The Salvation Army in Canada

"On behalf of the membership of the Montreal Council of Women (MWC) I wish to confirm our deep concern for those whose lives have been upended by having their images involuntarily and/or without consent shared on websites and other platforms such as the Montreal based PornHub. The proposed "Stopping Internet Sexual Exploitation Act" bill calls for much needed amendments to be made to the Criminal Code to protect children and those who have not given consent for their images and other content to be shared and commodified." **Penny Rankin, Past President, Montreal Council of Women** 

Parents Aware offers our full support on the Criminal Code amendments that are proposed in the Stopping Internet Sexual Exploitation Act. We feel that the addition of these offences with penalties is an effective way to hold companies and individuals criminally responsible when creating pornographic content depicting underage participants. Lisa Whitsitt, Director of Educational Outreach, Parents Aware

"There is not a more important piece of legislation to protect victims from criminal sexual exploitation online than mandatory age and consent verification for pornography production and distribution online. This is a long overdue, common sense, and urgently needed regulation that has the potential to protect thousands, if not millions of individuals, including children, from facing life altering, traumatic, sexual abuse."

Laila Mickelwait, Founder, Traffickinghub movement and CEO, Justice Defense Fund

"The pornography industry systemically fails to verify age or consent – leading to horrific trauma for survivors of sex trafficking, child sexual abuse, and non-consensually shared/recorded intimate images as their sexual exploitation is viewed around the world. It is time for a paradigm shift, and for survivors to be heard. This bill is an important step in that direction." Dani Bianculli Pinter, Senior Legal Counsel, National Center on Sexual Exploitation

From:	Eduard C. Dumitrescu ME ADDES:	510	Info
To:	ICN / DCI (PCH)		
Subject:	Having my say: The Government's proposed approach to address harmful content online		
Date:	September 8, 2021 9:45:29 PM		

Hi,

You put out a request for comments from all Canadians in https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html so I am responding as requested.

online is awful, for many reasons. Here are a few of them:

Your approach to harmful content s

s.19(1)

1. Anti-competition and anti-Canadian innovation: Expensive blocking filters and 24h response requirements means only very large corporations (Facebook, Google, Microsoft, etc) will be able to afford them.

2. Freedom of expression: The proposal attempts to ban "lawful but awful" speech. Focusing on the first part, this bill attempts to ban lawful speech on the internet. In an age of COVID19, people express themselves more and more via the internet. Do you want them to go outside and physically congregate with others to express their ideas?

 Undemocratic: Worse yet, the decision as to what's awful is mostly relegated to the Digital Safety Commissioner rather than a more varied sample (like the actual representatives).
 Dangerous: Next time the conservatives get elected (which might be soon if you keep pulling sh\*t like this), they will use this in all of the wrong ways. Like, they won't even pretend that this is meant to protect marginalized people or anything.

5. Ineffective for "offenders": China dumps a huge amount of money into their Great Firewall, and they still can't stop people from getting past it. Proxies, VPNs, anonymity networks, etc, are basically impossible to block. And they've been trying for a long time.

6. Ineffective for "victims": Trolls are clever enough to bait victims into getting mad and breaking the rules, resulting in victims getting banned instead. Trolls tend to have time to study the rules and prepare for their attacks, whereas their unsuspecting victims don't. The answer is to not try to have a gigantic platform try to regulate and host every possible type of speech, and let smaller platforms regulate themselves in ways that make sense for their demographics (their ACTUAL users). Arguably the de facto ban on small hosts is infringing on the right to freedom of association (but it's not unusual to break this one if you're also breaking freedom of expression).

We're in the middle of a pandemic, is a dead internet bill really what you want to spend time and taxpayer money on? That's lawful, but awful of you.

For more information,

https://doctorow.medium.com/canadas-got-the-world-s-worst-internet-ideas-e1ae6124db2a https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/

Best regards, Eduard Christian Dumitrescu

s.19(1)

 From:
 ICN / DCI (PCH)

 Subject:
 Sensorship

 Date:
 September 8, 2021 12:01:31 PM

If the Canadian Grubbment (government) can take away your right to say whatever you want to online. Whats next? The liberal government wants to sensor opinions that are not agreeable with their own in a shady attempt at staying in power longer.

Sent from my Galaxy

From:	Maximilian Sarte
To:	ICN / DCI (PCH)
Subject:	Digital Citizen Initiative - Comments
Date:	September 8, 2021 9:09:11 AM

Are you OUT OF YOUR FUCKING MIND!!!??? We certainly DO NOT NEED more censorship. We certainly DO NOT NEED CSIS in our lives. GET OUT OF OUR COMMUNICATIONS!!!! The current laws are restrictive enough to have more intrusion, censorship and pressure added on us. FUCK YOU!!! THE ANSWER IS NO!!! now and ever!!! SCRAP the whole idiotic idea!!! NOW NOW NOW

From:	Jason Withrow the Access to In
To:	ICN / DCI (PCH)
Subject:	Comments re "The Government's proposed approach to address harmful content online"
Date:	September 7, 2021 7:38:39 PM

As a Canadian citizen and voter, I oppose this framework in the strongest possible terms.

The framework includes extremely problematic proposals, including: p

- proactive monitoring of content;
- 24hr removal timeline (or face substantial financial penalties);
- MANDATORY OFFRAMP to law enforcement
- access to user information, along with a gag order;
- potential for ISP blocking by a regulator;
- pursuit of information related to software and algorithms

Along with others, I repeat that we are concerned there will not be a diversity of voices from experts who can speak to the unintended consequences on freedom of expression, political dissent and the potential implications on racialized and marginalized experiences.

These restrictions will harm the most vulnerable while leaving the guilty unscathed. Similar laws have failed over and over internationally and they will fail again here, at great cost to sex workers and the average Canadian. This proposal must be stopped before it is too late.

Sincerely, Jason Withrow

 From:
 Paul Wnuk

 To:
 ICN / DCI (PCH)

 Subject:
 Response Regarding New Approach to Online Content

 Date:
 September 7, 2021 7:24:35 PM

#### Good afternoon,

My name is Paul Wnuk. I'm writing to express my concerns about the new proposed framework to tackle harmful content online. This new approach would have a very negative affect on people who work in the adult industry.

Adult industry workers rely on online platforms to make a living. These laws could wind up banning adult workers from these platforms, leaving them unable to provide for their families. It may also leave them vunerable for arrest, making it harder for them to find another form of employment.

Adult industry workers have been having to deal with discrimination for years. The new laws for online content should put these people in mind so they don't have to worry about losing their main form of income.

Thank you,

Paul Wnuk

 From:
 General Email
 Me

 To:
 ICN / DCI (PCH)
 Me

 Subject:
 Government's proposed approach to address harmful content online

 Date:
 September 7, 2021 12:26:24 PM

No. Who will watch the watchers from pulling down items that aren't harmful but may be information that may not put the government in the best of light.

No again to all components of this ministry of truth. Under the guise of making our Internet more 'safe', a wide variety of lawful posts that online platforms choose to remove could soon be automatically reported to CSIS and the RCMP— with no rules whatsoever about what they do with that information!

From:	David Krae the Access to Information A
To:	ICN / DCI (PCH)
Cc:	mgelst@uottawa.ca; ann.cavoukian@gpsbydesigncentre.com; Info@freespeechcoalition.com; contact@sexworklawreform.com
Subject:	Digital Citizens Initiative - Harmful Online Content - Stakeholders and Canadians response
Date:	September 7, 2021 12:00:56 PM

Concerns:

Per the Technical Paper posted at the "Have your say" page at the Canadian Heritage website:

Were such a bureaucracy to be created, there are various structural problems with the proposed organization. The following are just a few of the logic problems at play and how it can be abused and cause tangible **\*harm**\* to individuals who fall subject to the proposed items:

26. Provision is made that "an OCSP must **\*NOT**\* disclose" but it does not appear to ensure that, after a period of time, OCSPs **\*MUST**\* disclose to the affected individual (the person or persons being investigated) that an investigation has occurred, or a report been issued.

This matters, because this proposed 'Digital Safety' regime will most assuredly be abused by activists, and potentially also business competitors. Certainly youtube creators have had difficulties with people falsely flagging their content. If a content creator is being targeted by repeated false reporting, they should be made aware of it. If a content creator is being investigated, they should also be made aware of it within a certain time period. And if a content creator has been investigated, they should be made aware of it within a certain time period.

Investigations **\*CANNOT**\* be open-ended, but could be extendible for reasonable periods under judicial restraint, from a judge familiar with the investigation – specifically the same judge who issued the first warrants obtained in the case, to ensure continuity of restraint.

If investigations involve "gag orders" and the contacting of associates of individuals under investigation, said individuals **\*MUST**\* be notified after a certain time period, regardless of the outcome of the investigation. Furthermore, any investigation that involves contacting other individuals associated with the individual or individuals under investigation, which is resolved without legal action or charges, must include **\*MANDATORY**\* follow-up with those individuals who were contacted and questioned, to inform them that the investigation was closed, with no impropriety found.

Such investigations are not only disruptive to people's business and personal lives, they can be damaging to their professional and personal reputations and relationships, and privacy, once lost is difficult, if not impossible to regain. RCMP, CSIS, Police and any other investigative officers, cannot be permitted to call a person's integrity into question (damage which occurs from the very act of investigating a person) without ensuring that reputational integrity is restored, should an investigation be a false alarm.

### Document communique en vertu de la Loi sur l'accès à l'information. Document released pursuant to

Much ado is made about the timeliness by which OCSPs must report, take action, and respond to flags, but very little attention given to the timeliness of RCMP, CSIS and other agency investigations. These **\*MUST**\* require a warrant, issued by a judge, with a reasonable time limit on said warrants, and any renewals or extensions **\*MUST**\* be acquired from the same judge, to ensure continuity and legal integrity of the judicial oversight.

#### Module 1(C)

35. a) Section II demonstrates that the proposed legislation has a specific agenda, to suppress political speech and Freedom of Expression, by expanding definitions of 'hate speech' to include free and open political discussion and debate of societal and political issues pertaining to special-interest groups itemized. Especially considering how activists are now framing the concept of "harmful content" as anything that doesn't automatically capitulate with the demands of those activists, abuse of the Digital Safety Commission and its powers to suppress the political and cultural Speech and Expression of Canadians is all but guaranteed.

Politicizing the legislation in such a way is a clear indication that it will be used politically, especially considering how much Canadian political speech and socialization occurs via online platforms in the 21<sup>st</sup> Century.

43. What is the purpose of this provision? If a "hearing" is required, that is a matter for the courts to decide. Otherwise, the Digital Safety Commissioner – a political appointee – will be in the business of disrupting speech, destroying businesses, and destroying reputations, as well as publicizing people's personal information in regard to a matter that is not worthy of criminal charges – all on its own 'discretion' of what is in the "public interest". Given the already-existing reporting regime of the courts, provision 43 is unnecessary and too easily abused. Same as 53.

46. The Digital Recourse Council (DRC) should **\*NOT**\* be appointed by the Governor in Council, since that same office also appointed the members of the Digital Safety Commission. The DRC **\*SHOULD**\* consist of individuals who are knowledgeable about the law, and Canadian Charter Rights. The members of the DRC, whose job it is to protect Canadians and their Charter rights from abuse by the politicized office of the Digital Safety Commission (DSC), should be appointed by multi-partisan committee comprised of Members of Parliament. If the point of a DRC is to counterbalance the powers DSC, then do that, otherwise the DRC is nothing more than an empty, rubber-stamping office, and an excuse for political insiders to give an easy paycheck to a group of their pals.

Furthermore: It should be stipulated that nothing in the Act should preclude Canadians from having the right to sue the Canadian Government for abuses and disruptions of their businesses and Charter protected rights by the Digital Safety Commissioner. Also, the records of complainants should also be preserved, so that any individual affected by the complaints can pursue civil recourse if complainants are systematically targeting them.

83. Is problematic in that same regard.

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

87. No sharing of information with foreign entities without judicial review. ess to information Act

89. That section is almost verbatim cut-and-paste from the Conservative Bill C-30, including the use of the term 'Inspector' – and should not be permitted without a search warrant issued by a judge.

94-109 – The entire concept of **\*Administrative Monetary Penalites (AMPs) should be <u>struck</u> <b>entirely\***. If there is a criminal matter at hand, refer it to the courts. Period. Otherwise, what you have created with the Digital Safety Commission, is nothing more than a Politburo.

CSIS Act – Just get warrants. They are easy to get from judges, especially if there is potential child abuse involved.

#### **General Comments / Summary**

The 'Harmful Online Content' bill is unnecessary overreach, and, as proposed, it represents an attack on Canadians' Charter Rights and Freedoms, as well as having a chilling effect on political, social, cultural and artistic expression of individual Canadians, their professional and private reputations, and livelihoods.

You could have accomplished this much more easily and far more cost-effectively if you had simply indemnified Canadian OCSPs from financial harm for temporarily suspending suspected unlawful content for a period of 72 hrs for review, if a complaint is made, and reporting to legal authorities if necessary. Also, Cybertip, the Internet Watch Foundation, and other similar organizations already exist and concert efforts worldwide, to determine if content is unlawful and refer cases where it is, to the legal authorities in the appropriate jurisdictions. Instead of creating an unnecessary, costly, and Orwellian government agency like the Digital Safety Commission ( -- as the Technical Paper describes, it is effectively a Digital Secret Police) award more resources to those organizations already doing good work, and let the existing legal authorities investigate where warranted.

A major problem also ignored here is the often false and fraudulent activism by organized political groups, who will use these 'proposed' measures to suppress Canadians' Charter Rights and Freedoms. There are already questions about the honesty and integrity of the testimony of individuals associated with organizations like Exodus Cry, NCOSE (formerly known as Morality in Media) and Traffickinghub, which appear to be primarily religious activists, using the issue of CSAM as a wedge issue to push for the effective ban of all adult content entirely, which is what the proposed legislation will effectively do.

Considering the way the proposed Digital Safety Commission is constituted, it will provide those same activists, and activists on other topics, cultural and political, with easy mechanisms to "chill" and shut down Canadian Freedom of Expression entirely, by intimidating OCSPs and Canadian individuals from expression.

If such a frankly unnecessary bureaucracy as the Digital Safety Commission is created, it will most assuredly be abused by unethical activists, to suppress the speech, expression, and political participate of Canadians. Ultimately, what is being proposed, is very little different from the aborted

### Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

Bill C-30 proposed by the Conservative Harper Government and put forward by Vic Toews in 2012 — A CA and, worse, it will definitely be politicized and abused by whatever government is in power, groups that hold cultural hegemony, and people willing to lie and game the system being created, to suppress the political speech of whoever is not, and that includes many minorities, and people in careers where their safety is tied to their privacy.

There are far better ways to go about dealing with issues of CSAM, without creating what is functionally a Politburo and Secret Police, and without infringing upon and intimidating platforms where Canadians engage in their Charter Rights and Freedoms. Also, perhaps consider what such an organization can be used for in the hands of other political parties, for their agendas. In fact, all politicians should consider what their political rivals would do with such powers, whenever considering whether to create and award such powers to themselves. And how soon before Canadians tire of the current party in power and vote them out, just for a change, as is common custom?

Thank you for your time and attention to this matter.

Respectfully,

David Krae – Author and Filmmaker

 From:
 Cassie L

 To:
 ICN / DCI (PCH)

 Subject:
 criticism of the new "harmful content" ideas

 Date:
 September 7, 2021 9:55:10 AM

You guys should take very seriously what is being written about by https://techpolicy.press/five-big-problems-with-canadas-proposed-regulatory-framework-forharmful-online-content/ She talks about many things that I couldn't speak on better than she does.

As for my personal experience, I have some worries there too. I run a platform in Canada where sex workers post adult videos of themselves to sell. I currently go above and beyond the required measures to make sure the people selling the videos are the people in the videos and that they are old enough and consenting. I personally look at all the content before it goes live and speak with each model and I turn down studios who want to sell videos because I value the success of independent sex workers FIRST and know how much studios take advantage of people sometimes.

Even on a platform like mine it will be difficult to take down any video flagged by an algorithm within 24 hours. Certainly when I think of the models that work with my platform, I know they would not be online and reachable to take down videos on twitter flagged by the algorithm within 24 hours. It's funny when I think of how sites will be forced to take SWIFT action on videos flagged by a robot that might be fine, but sex workers who are reporting their content stolen and published or sold without their consent can't get it removed from websites ignoring or immune to DMCA (or canadian equivalents) takedown requests. God forbid one of these women doesn't want to give her FULL LEGAL NAME AND ADDRESS in order to ask politely for her revenge porn to be removed. Surely someone posting revenge porn would not misuse that sort of information right? There is no required firm timeline for DMCA takedowns let alone 24 hours.

Also algorithms are NOTORIOUSLY flawed and will falsely flag MANY things - likely primarily targeting marginalized and racialized groups since algorithms trained on a flawed society absorb and perpetuate those flaws. It will miss everything on the dark web and will make totally safe online sex work much more dangerous, just like sesta/fosta did.

Please consult many sex workers when proposing things like this.

'Cassie' AKA

s.19(1)

From:	Grant Willison
To:	ICN / DCI (PCH)
Subject:	The Government's proposed approach to address harmful content online
Date:	September 2, 2021 11:35:19 AM

Hello;

Thank you for providing citizens an opportunity to contribute to the Digital Citizen Initiative.

I have read the proposed legislation regarding harmful online content, and I must say that the legislation is horrible. It chooses to place the onus on ISP providers, whom have a sole purpose to increase revenue for their shareholders.

It also has a "czar" to determine what is appropriate speech, but it well established that this style of approach consistently marginalizes those segments of our citizens already marginalized.

The primary author should be relieved of this responsibility. World leading experts such as Dr. Michael Geist should be leading a document such as this. To not put the most skilled people in charge of this very important endeavor is prideful and foolish.

The current proposal, as presented currently, only drives people to vote for non-liberal candidates. Truly it is that bad.

Best regards,

Grant Willison

From:	Yagya Parihar
To:	ICN / DCI (PCH)
Subject:	Re: The Government's proposed approach to address harmful content online
Date:	September 5, 2021 9:01:53 PM

To whomever it may concern,

As a Canadian citizen, I am concerned with elements of the proposed law framework for social networks and ISPs. I would like to point out some areas where I believe there are problems.

The primary problem is the content flagging mandate, as shown below:

The new legislation would set out a statutory requirement for regulated entities to take all reasonable measures to make harmful content inaccessible in Canada. This obligation would require regulated entities to do whatever is reasonable and within their power to monitor for the regulated categories of harmful content on their services, including through the use of automated systems based on algorithms.

Such flagging of content would require automated filters, since any other method of filtering would be unreasonable, especially given the amount of data uploaded to such networks. As an example, as of 2019, YouTube had 500 hours of content being uploaded each minute (source). Automated systems are known to disproportionately target minority groups, which is an especially large issue considering that these proposed regulations aim to protect such people. This report shows the problem with false flagging of accounts.

Such automated flagging also affects completely innocuous content, in what is known as the Scunthorpe problem. The Wikipedia page on the problem links to sources of various instances of this happening.

Beyond that, I believe that three of the categories of content that are covered are quite broad.

The legislation would target five categories of harmful content:

- · terrorist content;
- · content that incites violence;

The word 'terrorist' is a very subjective word that does not have a definite meaning, and can be used as a characterization, as shown in this article from The Guardian, and is brought up in this report from the US state of Arizona's Department of Emergency and Military Affairs. "Content that incites violence" can also easily be taken as anything that criticizes the government.

· hate speech;

The already unclear definition of hate speech is magnified here, and given the scale of the Internet, attempting to automatically filter hate speech would again result in innocuous speech being caught.

Once platform users flag content, regulated entities would be required to respond to the flagged content by assessing whether it should be made inaccessible in Canada, according to the definitions outlined in legislation. If the content meets the legislated definitions, the regulated entity would be required to make the content inaccessible from their service in Canada within 24 hours of being flagged.

A 24-hour content flagging period exacerbates the problems brought up earlier, as with the scale of content being uploaded, the 24 hour period would simply not be enough.

One approach would be to require that regulated entities notify law enforcement in instances where there are reasonable grounds to suspect that there is an imminent risk of serious harm to any person or to property stemming from potentially illegal content falling within the five categories of harmful content. In this approach, "imminent harm" and "serious harm" are high thresholds that would need to be defined. Even if noticeably illegal content is likely to lead to violence or terrorist activity, there would be no obligation to report such content to law enforcement or CSIS.

While this is the ideal approach to take in such a situation, as stated earlier, the 24 hour period is not enough to make decisions on such content.

Another approach would be to require that regulated entities report certain types of potentially criminal content directly to law enforcement and content of national security concern to CSIS. This reporting obligation would only apply to prescribed content falling within the five categories of regulated harmful content. The legal thresholds (reasonable suspicion, reasonable grounds to believe) for reporting this content would be prescribed by the Governor in Council and could differ based on the category. For example, the threshold for reporting potentially terrorist and violent extremist content could be lower than that for potentially criminal hate speech.

Direct reporting of content would lead to larger problems for Canadian citizens, especially with an algorithm vetting content, as that would result in many false reports and the resources of Canada's police and judicial system being wasted.

#### Another issue is this:

The Act should provide that an inspector may enter, at any reasonable time, any place in which they believe on reasonable grounds there is any document, information or any other thing, including computer algorithms and software, relevant to the purpose of verifying compliance and preventing non-compliance with the Act, regulations, decisions and orders, and examine the document, information or thing or remove it for examination or reproduction, and: • make use of, or cause to be made use of, any computer system at the place to examine any data contained in or available to the system;

• reproduce any document, or cause it to be reproduced, from the data in the form of a print-out, digital copy, or other intelligible output and take the print-out,

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

digital copy, or other output for examination or copying; and coess to information Act. • use any copying equipment or means of communication in the place.

Allowing for such searches is an invasion of privacy. The personal electronic devices and software of a user contain as much private information as their home does, and as a result should be subject to the same protections, as mentioned below:

The Act should provide that an inspector may not enter a dwelling-house without the consent of the occupant or under the authority of a warrant.

I would recommend reading this article from the Electronic Frontier Foundation and reconsider this decision.

Yagya Parihar

From:	Eric Lindgren
To:	ICN / DCI (PCH)
Subject:	Harmful content legislation
Date:	September 4, 2021 1:25:13 PM

Re: Government's proposed approach to address harmful content online

So far what you're proposing is too invasive without enough counterbalance. I would strongly urge you to reconsider and to listen to experienced critics such as the Electronic Frontier Foundation in the United States.

At present what you're proposing is un-Canadian in a very deep and disturbing sense.

-Eric Lindgren

From:	Kyle Nicol (DE
To:	ICN / DCI (PCH)
Subject:	Government's proposed approach to address harmful content online
Date:	September 5, 2021 1:09:18 PM

#### Hello,

I am writing in regards to the new legislation being proposed by the Liberal government to address "harmful content online"

These proposals are terrible to put it bluntly. There doesn't appear to be any regard paid to net neutrality or an open internet for everyone, despite the Liberal government's claims to support those ideals. It seems like it will punish everybody except for the largest companies like Facebook, Twitter, TikTok, Instagram, and all the major social media platforms that seem to be the targets of these proposals, because they will be able to easily afford any penalties they will have to pay. Anybody who can't can easily just stop operating in Canada or let these idiotic rules force Canadian ISPs to block their sites. This will limit what is available to Canadians to only those that can afford to do whatever they want anyway.

Additionally, the idea that the government will force ISPs to block certain websites because of whatever they deem to be "harmful" content is ridiculous. What is considered harmful content by today's government can easily be changed when a new government comes in to power. I'm sure certain things the Conservatives (or, god help us, the People's Party of Canada) would consider "harmful content" would not be thought of the same as the Liberal party. I wonder why I haven't heard Justin Trudeau touting these new proposals on the campaign trail? Nobody would be in favour of these, nobody wants these, and they would be met with derision and anger.

Canada deserves people in charge who actually understand technology, computers, and the internet. We also deserve a government that actually stands up for net neutrality and having an open and fair infrastructure for all it's citizens. That would be better than the current government, who caters to the big 2 companies, Bell and Rogers, letting them dictate whatever they find in their best interests. I assume that within a few years these proposals would also include content that they would deem "harmful", that is content that infringes on their ways to make money.

I don't expect anything to come of this because it is clear that this government does not care about what it's citizens thinks about these proposals.

With disgust,

Kyle Nicol

From:	Jeanette Schwarz
To:	ICN / DCI (PCH)
Subject:	Censorship of the internet
Date:	September 3, 2021 4:10:11 PM

Hello,

I have noticed censorship of the internet, especially around discussion around the vaccine passports. I do not agree with this.

<u>Discussions</u> around important topics are necessary, and censorship is on sided propaganda. Please stop censorship and one-sided information online. Thank you.

Sincerely, Jeanette S.

 From:
 Martin Duhamel

 To:
 ICN / DCI (PCH)

 Subject:
 feedback for digital citizen initiative

 Date:
 September 1, 2021 2:40:56 PM

 Attachments:
 Letter to Digital Citizen Initiative.pdf

Hello,

Please find the attached letter.

RE: Government's proposed approach to address harmful content online

Martin Duhamel

s.19(1)

s.19(1)

September 1, 2021

By email: pch.icn-dci.pch@canada.ca

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St. Gatineau QC K1A 0S5

#### RE: Government's proposed approach to address harmful content online

In response to your request for submissions, I would like to suggest that you change the name "Digital Safety Commission" to "Social Media Standards Commission."

The reason for this suggestion is that the word "safety" does not capture the essence of the Commission's mandate, and it is misleading about what the public should expect from it.

With regard to curtailing "hate speech," even a success in this matter would not make social media "safe" for the user. There would continue to be disagreeable people and unpleasant content that falls short of Canada's legal threshold of "hate." The government cannot deliver "safety" from offensive content because people vary widely in what they consider offensive. Of course, it would still be useful to have content warnings (as we have on movies and TV shows) so that adults can choose what they want to see, and so that children can be restricted from viewing certain materials.

With respect to child sexual exploitation content, your principal concern is not the "safety" of the social media user. Your concern is the mitigation of the abuse that has already occurred, and the stopping of the spread of images. The prevention of *further* harm does not suddenly make the abuse victim "safe." Neither of these goals falls under the rubric of "safety."

With respect to terrorist content, your principal concern is, again, not the "safety" of the social media user. If the Commission is successful, it might have contributed to reducing societal strife, but its role is far-removed from any actual harm that might have occurred at a later date. Granted, I do not want to accidently see a beheading video, so I would appreciate a content warning. But the problem of ISIS propaganda is trivialized by considering it a matter of "public safety."

With regard to content that incites violence, your principal concern is (for the third time) not the "safety" of the social media user. Inciting violence is itself a crime, and the Commission would have a role in responding to that crime, but it would be far-removed from any eventual physical conflict. It is incorrect to characterize the Commission's role as one of "safety." 'Crime' and 'safety' are not antonyms. The Commission's anti-crime role is not a "safety" role.

With regard to the non-consensual sharing of intimate images, your goal is (for the fourth time) not the "safety" of the social media user. Moreover, the Commission's role in the reduction or prevention of harm is not equivalent to creating "safety" for the person who was photographed.

There are laws against theft. Does this mean that we're all "safe" from thievery? Not at all. Analogously, the laws you're proposing are not about achieving safety.

Safety is achieved by, say, erecting a guardrail. But if something has already gone off the edge, "safety" is no longer the relevant issue. None of the issues contemplated above, with the exception of content warnings, are properly characterized as "safety." They are reactionary, not anticipatory. You are not mandating anything that could be likened to seatbelts or to consumer product testing and certification.

"Digital Safety Commission" is a name that a politician would like. Nobody's against safety, right? However, saying "safety" is wrong, and it misleads the public in a way that is discreditable to the public servants who will create and run the institution. The name "Social Media Standards Commission" is correct and it doesn't patronize or infantilize the public. "Online Content Standards Commission" is another option.

Thank you for considering this suggestion. This is just one of many issues to which I hope you'll give further consideration.

Sincerely,

Martin Duhamel

s.19(1)

From:	White, Patrick MELADCESS	
To:	ICN / DCI (PCH)	
Cc:	White, Patrick	
Subject:	Commentaires sur l'approche visant à lutter contre le contenu préjudiciable en ligne	
Date:	September 1, 2021 2:35:52 PM	

Bonjour,

J'ai l'impression que mon commentaire ne s'est jamais rendu.

Voici mes 2 commentaires sur votre politique contre le contenu préjudiciable en ligne.

Je suis favorable au projet globalement.

Mais il y a 2 problèmes majeurs :

- La définition du contenu haineux doit être hyper précise sinon bien des groupes religieux pourraient assimiler l'humour et la critique de leur religion comme étant du contenu haineux ou des attaques haineuses. Ceci pourrait nuire grandement à la liberté d'expression des Canadiens et des médias
- La politique doit aussi s'appliquer aux messages instantanées comme Facebook Messenger, WhatsApp, Telegram ou Signal, qui sont de très grands vecteurs de contenu haineux, de propagande, de Fausses nouvelles et de désinformation,

Cordialement,

Patrick White Professeur de journalisme, UQAM Université du Québec à Montréal (UQAM) (514) 779-5680

From:	Brian Probert
To:	ICN / DCI (PCH)
Subject:	Address harmful content
Date:	August 31, 2021 1:42:31 PM

#### Hello,

I'm extremely concerned by this proposal, as anyone who values democracy should be. This has massive potential for government over-reach and censorship of views or discussions it seems to be "harmful". This could easily be interpreted to including dissent against government policies, passionate frustration with the leading party, or even just any conversations and ideas the government decides it believes to be "harmful".

Censorship such as this has destroyed the freedoms and ability to discuss important issues relating to the country in places like China and nobody in Canada wants our government to have the same heavy handed control over our speech and what can be seen on the internet as China. It's extremely troublesome to even have a proposal like this being considered in Canada, when the very groups and hateful content it's presented as being to enforce, are already illegal and already have mechanisms to remove and investigate.

These new proposals are just another example of false fears spread in order to give more powers to the government to silence critics and shape the narrative into one it views more favourably, and any groups who dabble in illegal or extremist content have many, many options for ways to continue these things out of the view of these proposed regulations, and they will primarily be used against every day people, having lawful discussions and covering topics that may not be what the government wants us to discuss, such as their own illegal or scandalous misdeeds.

The best way to counter ideas we deem to be harmful, misinformation or concerning is by allowing the open dialogue, so we can truly understand where these views are coming from, and properly address the concerns through understanding, education and information. You will never stop any of these conversations and views without changing the minds of the people who carry them, and unless we can be allowed to discuss and discredit these ideas, we will create even more extreme, and more underground groups who isolate themselves into secure echo chambers where there is no hope to resolve their issues or address their concerns. This will lead to an invisible army of extreme groups, hidden from public and government view until they decide to take action.

We cannot allow this type of thing to happen, and it will. Criminals and extremists are always one step ahead of the government, and they will easily find alternative locations to espouse these "harmful" ideas, discretely hidden away where they cannot be countered or even acknowledged, so no one will even know about this segment of the population in order to be able to counter them and discredit them.

I have zero support for government censorship or regulation of the internet. You will kill rational discussions where extreme or harmful ideas can potentially be reformed and you will bury these ideas into the deepest darkest areas until they grow to be too large to reform. Everyday citizens do not deserve to be censored or have their internet regulated into whatever the governments accepted narrative or image is.

It may seem like a temping idea when the leader who you deem to be the "good guy" has these powers to silence people you deem to be "bad". As we have seen around the world, the "good guys" don't always remain in power and we can be opening the door to even further totalitarian and dangerous controls of speech and freedoms than already exist.

From:	tammy browder (NELACC	
To:	ICN / DCI (PCH)	
Subject:	Re: The Government's proposed approach to address harmful content online	
Date:	August 30, 2021 11:06:20 PM	

I am concerned that this is a backdoor to Bill C-10. The sentiment is good, but free speech still needs to be preserved. We have existing laws against hate-speech. But not everything, is motivated by hate or the desire to destroy others. Sometimes there is simply disagreement. Who will decide what online content is "harmful?"

By continually silencing these alternative opinions, these proposed "approaches" are simply damaging Canada's credibility and trust with its own citizens. It's tragic and very frustrating to see a new face of this doomed, destructive endeavour being pushed in the interest of what I feel are powerful, covertly operating special interest groups.

 From:
 Erank Butler

 To:
 ICN / DCI (PCH)

 Subject:
 Harmful online content filtering

 Date:
 August 30, 2021 7:14:33 PM

As a Canadian citizen and taxpayer, I reject this wholeheartedly. Wrong approach and will cause more harm than good. Pls rethink this and come up with a better solution.

Thanks! Frank Butler

From:	Ashley Rourke
To:	ICN / DCI (PCH)
Subject:	Stop censorship
Date:	August 30, 2021 4:01:54 PM

I am asking that you to put a stop to what you are doing with this censorship, every mind has an opinion and right to share. You CANNOT pick and choose what information is being shared for the benefit of the government as you are creating an ugly world putting individuals against one another where it would normally NEVER happen. Who says what your allowing to be shared on main stream media is correct? Why haven't people been able to hear from the MANY doctors and science professionals opposing the information on COVID posted all over the news? Why allow media to target the unvaccinated knowing full well that the vaccinated are able to contact and spread the virus just the same as those not vaccinated? We should ALL be able to access information from BOTH sides in order to make informed disiourselves. I am a concerned citizen that pays my taxes and abides by all the rules except this, this is all about control. I will always take a stand for what I believe and I believe that the world is being misinformed. Save our people, save our world, stop the poison.

STOP CENSORSHIP! LET PEOPLE LIVE! STAND FOR FREEDOM OF CHOICE.

Get Outlook for iOS

s.19(1)

 From:
 Ralph Haygood
 Strotty
 ME ADDESS TO

 To:
 ICN / DCI (PCH)

 Cc:
 Subject:
 comment on the government"s proposed approach to address harmful content online

 Date:
 August 30, 2021 5:00:19 AM

 Attachments:
 comment by ralph haygood.pdf

To whom it may concern:

The PDF file attached to this message contains my comment on the government's proposed approach to address harmful content online, per

https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html

The comment is also available as a web page at

https://ralphhaygood.org/harmful\_online\_content/comment.html

I also plan to send the comment to selected Members of Parliament, journalists, and other potentially interested parties.

Ralph Haygood

 From:
 Jean-François Poirier

 To:
 ICN / DCI (PCH)

 Subject:
 Wrong-headed approach to social media harmful content

 Date:
 August 28, 2021 10:45:05 AM

#### Greetings;

As a long-time Internet user (I gained Internet access in 1989) with a strong, long-standing interest in its effects on society and culture, I have watched the federal government's (misguided) efforts to attempt to control the flow of cultural production (commercial and individual) with increasing dismay.

The government has obviously not taken the time to look at historical precendents (DMCA, SESTA-FOSTA, etc) – legislation intended to provide government-based control on decentralised artefact production (software and hardware for one, content for the others), with disastrous results.

DMCA was co-opted by businesses to create an artificial lock on competition, valid scientific research and cultural production. SESTA-FOSTA ended up penalising and silencing valid discussions surrounding sex work and sexual content.

It's already bad enough that companies like Facebook, due to their prominance and cost of switching out, become \*monopolies\* that get to be censors by default of our content (removing such culturally vital and historically informative works such as the painting "L'origine du monde" but leaving in full-view \*MARJORIE GREEN TAYLOR\*, not to mention livestreaming of incredibly damaging content comes to mind), but government control of their behavior is \*not\* the answer.

The goverment will \*NEVER\* be fast enough or knowledgeable enough to keep up with the hyper-rapid changes and adaptations of companies as big as Facebook, whose revenue and operations dwarf its own capabilities. To think that it can draft and maintain rapidly enough a legal framework to shape its output is not only fallacious, it is destined to end in catastrophe.

The issue with these platform is not one of control, it is one of sheer size, and \*monopolistic tendencies\*. You don't fix monopolies by telling them their business model needs government control (which is in essence what any federal framework on the content of such businesses platform turns into), you fix them by TURNING OFF THEIR MONOPOLY SITUATION.

 Break them up - Facebook owns too many channels and too much marketshare, acquired by ingesting competitors and giving it an unfair hand in everything. Even right-wing competitors cannot start alternative services that survive.

2. Enforce a mandate to let people \*leave\* -- why is Facebook so strong? There are no competitors. Why are there no competitors? Because people wouldn't leave for them. Why do people not leave? Because everyone is on Facebook. Why is everyone on Facebook? Because you \*can't leave\* -- there is \*no\* possibility to migrate your data

somewhere else, or no possibility for other services to connect/interoperate with them, effectively locking its customers inside a walled garden. THIS gives it unnatural power.

It is not by trying to label/filter content that the amount of garbage on the networks will change -- Facebook THEMSELVES showed that this is an IMPOSSIBILITY to achieve - if anyone has the resources and power to do it, they do. And they have repeatedly failed in this.

If they cannot do it themselves when their business would benefit from such a process (YouTube tried, unsuccesfully, and so did Facebook), how would a governmental mandate \*demanding\* a snake oil solution fix anything?

Michael Geist has repeatedly documented the horrifying approach of our current federal government to addressing technological monopolies by focusing on their output rather than their corporate structure/market position, which is assuredly looking at the wrong end of the telescope.

Not only that, but ANY GOVERNMENTAL CONTROL MANDATE WILL RESULT IN DANGEROUS, CONCENTRATED REPOSITORY OF PERSONAL IDENTIFYING INFORMATION. In 2021, with every bloody example of the impossibility to protect such repositories and the concensus in the security community on the toxicity of centralised repositories for PII, for the Liberals to suggest such an approach is either unacceptably naive, or purely incompetent.

This legislative effort NEEDS to stop. Look at the BUSINESSES -remember that hate speech is not GENERATED by them, but by the very canadians that elect them; this is not 1984, once cannot silence them, only reduce their impact by reducing their reach, by reducing the power of their conduit.

Look at these business as megaphones. The more of them there are, the less impact a single one them has.

THAT's the way to fix this.

Cory Doctorow, a luminary (and Canadian) on this topic, says it best: https://pluralistic.net/2021/08/11/the-canada-variant/#no-canada

Get this right, because the impact on Canadians can be devastating, and last for waaaay too long.

Jean-François Poirier Cloud security architect/Operations Manager

 From:
 INFO/INFO (PCH)

 To:
 ICN / DCI (PCH)

 Subject:
 FW: Have Your Say document feedback

 Date:
 August 26, 2021 8:23:03 AM

Hello,

We received the email below from Carole Telman regarding harmful content online.

Thank you!

## **Client Service and Public Support**

Department of Canadian Heritage | Government of Canada <u>PCH.info-info.PCH@canada.ca</u> Telephone (toll-free) 1.866.811.0055 TTY (toll-free) 1.888.997.3123

## Service à la clientèle et soutien au public

Ministère du Patrimoine canadien | Gouvernement du Canada <u>PCH.info-info.PCH@canada.ca</u> Téléphone (sans frais) 1.866.811.0055 ATS (sans frais) 1.888.997.3123

From: Carole Telman Sent: August 25, 2021 8:03 PM To: INFO/INFO (PCH) <PCH.info-info.PCH@canada.ca> Subject: Have Your Say document feedback

s.19(1)

Note: At the last observation I make, I see something constructive and feasible in your document. I hope you will read to the end to catch that.

## My feedback is in red font:

The Government believes in supporting a safe, inclusive, and open online environment. In partnership with the Ministers of Justice and Public Safety, the Minister of Canadian Heritage is publishing a detailed technical discussion paper that outlines the Government's proposed approach to regulating social media and combating harmful content online.

## Whereas:

1. Laws already exist against "inciting to violence against identifiable groups" and "promoting violence against identifiable groups" in the Criminal code.

2. There are also laws regarding the threat of violence against individuals already in the Canadian Criminal Code.

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

3. People should understand that they choose to expose themselves to questions or ACL criticism when they express something on a public forum.

Needed:

1. An objective and universal definition of "harmful."

2. Clear connections to any relative articles in the Canadian Criminal Code.

3. A list of specific terms related to an act of "harm" that would stand up in a court of law and that could be recognized and cited through an electronic algorithm and could not be overridden by adding replacement terms in the vocabulary.

4. Reminders by the social media platform to remind the poster and commenter in a pop-up of any related Canadian Criminal Code so the poster can submit a complaint to law enforcement and/or the commenter can retract the comment.

This approach is based on extensive work that the Government has conducted over the last year. It reflects consultations with equity-deserving communities, Indigenous organizations, non-governmental organizations, and victims of hate speech.

Whereas:

1. Within the proposed Bill C-36, the words "detestation or vilification" are given as definitions for "hate speech."

2. Detestation is a motivation-based word that can be laid upon someone unfairly and is difficult to prove in a court of law.

3. This "Have Your Say" process itself exists because the Canadian government considers harmful speech "vile, morally depraved, ignoble, wicked, disgusting, or repulsive" and is trying to censor people who call something "vile, morally depraved, ignoble, wicked, disgusting, or repulsive."

4. Comments or opinions can enter the realm of liable, for which there are already mechanisms in the law. If someone is accused of being vile, thereby damaging their reputation, and they are not, they can seek legal recourse.

Needed:

1. Either:

a. A simpler definition of hate speech to that of "vilification."

b. A dual definition like the proposed Bill C-36 uses but with a second nonmotivational and more descriptive word like "vilification."

It draws on insights shared by civil society and advocacy groups across the country. And it balances perspectives and approaches developed and shared by Canada's partners across the globe.

The difficulty with these goals:

Even if it were possible to develop and share a perfect balance of perspectives and approaches in media flatforms such as bookstores, libraries, television, radio, the internet,

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

or social media, it is impossible to control the consumption of those offerings in a free from Act society. People will consume only what interests them.

Needed for Clarification.

- 1. A list of "Canada's partners" being referred to here.
- 2. Clarification on how such "partnerships" exist and work.

The Government intends to introduce a bill in the fall of 2021. This consultation is an important step to provide Canadians and stakeholders with the opportunity to better understand the proposed approach and for the Government to consider additional perspectives.

This bill will be part of an overall strategy to combat hate speech and other harms. As part of this overall strategy, the Government introduced <u>Bill C-36</u> on June 23, 2021 to provide legal remedies for victims of hate speech and hate crimes. Bill C-36 proposes to:

- amend the <u>Canadian Human Rights Act</u> to enable the <u>Canadian Human Rights</u> <u>Commission</u> and the <u>Canadian Human Rights Tribunal</u> to intake, review, and adjudicate hate speech complaints; and
- amend the <u>Criminal Code</u> to provide a definition of 'hatred' for the <u>section 319 hate</u> propaganda offences and create a new peace bond designed to prevent the commission of hate propaganda offences/hate-motivated crimes.

Difficulty with this last goal:

It is not possible to omnisciently, fairly, or legally, charge someone with an emotion (*i.e.* hatred), only with an action or expression of speech. For the latter, the action would need to be recognizable with a clear list of words or phrases. Even then, new words and terms can easily be created over time to replace what is currently being used.

<u>Bill C-36</u> would complement the regulatory approach for online social media platforms that is proposed here.

Social media platforms and other online services help connect families, friends, and those with common interests in Canada and around the world. They are key pieces of economic infrastructure that enable Canadian companies to reach domestic and foreign markets, and are particularly crucial for small and medium-sized enterprises. They provide space for people in Canada to participate in their democracy, and for activists and civil society organizations to organize and share their messages, and amplify the voices of underrepresented and equity-deserving communities, including Indigenous Peoples.

Whereas:

1. Social media platforms "help [people] connect [with] those with common interests."

2. Social media platforms "provide space for people in Canada to participate in their democracy."

3. Social media platforms can theoretically "help... amplify the voices of underrepresented and equity-deserving communities, including Indigenous Peoples."

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

4. The services described in the above are currently provided by allowing people to On Act choose those with whom they will connect.

Needed:

1. A recognition that there is nothing in the mission statements of any social media platforms by which they commit to "amplify the voices of the underrepresented", etc. In other words, an honest understanding of the original intentions when social medias were developed rather than imposing tasks on them that they never promised to provide is needed.

2. The continued freedom for people to connect and participate as listed on social media.

3. An understanding, again, that people inevitably expose themselves to questions or criticism when they express something on a public forum.

But a growing body of evidence shows that these benefits also come with significant harms.

Individuals and groups use social media platforms to spread hateful messaging. Indigenous Peoples and equity-deserving groups such as racialized individuals, religious minorities, LGBTQ2 individuals and women are disproportionately affected by hate, harassment, and violent rhetoric online. Hate speech harms the individuals targeted, their families, communities, and society at large. And it distorts the free exchange of ideas by discrediting or silencing targeted voices.

## Whereas:

1. The term "discredit" is not the same as questioning logic or evidence behind what is being posted.

2. There is an assumption that "silencing" is not meant to be taken literally (eg. making a person physically mute, crippling someone so that they are unable to compose a piece of literature, etc).

## Needed:

1. A clear definition of "discredit" that would stand up in a court of law, that differs from slander or liable which are already addressed in Canada's Criminal Code, that could be recognized and cited through an electronic algorithm, and that could not be overridden through the addition of new terms and phrases to the vocabulary.

2. A similarly clear definition for the word "silencing."

Social media platforms can be used to spread hate or terrorist propaganda, counsel offline violence, recruit new adherents to extremist groups, and threaten national security, the rule of law and democratic institutions. At their worst, online hate and extremism can incite real-world acts of violence in Canada and anywhere in the world, as was seen on January 29, 2017 at the Centre culturel islamique de Québec, and on March 15, 2019, in Christchurch, New Zealand.

Social media platforms are also used to sexually exploit children. Women and girls, predominantly, are victimized through the sharing of intimate images without the consent of the person depicted. These crimes can inflict grave and enduring trauma on survivors, which is made immeasurably worse as this material proliferates on the internet and social media.

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

Social media platforms have significant impacts on expression, democratic participation, national security, and public safety. These platforms have tools to moderate harmful content. Mainstream social media platforms have voluntary content moderation systems that flag and test content against their community guidelines. But some platforms take decisive action in a largely ad-hoc fashion. These responses by social media companies tend to be reactive in nature and may not appropriately balance the wider public interest. Also, social media platforms are not required to preserve evidence of criminal content or notify law enforcement about criminal content, outside of mandatory reporting for child pornography offences. More proactive reporting could make it easier to hold perpetrators to account for harmful online activities.

Whereas:

1. Social media outlets are not required to report or preserved evidence of criminal content.

Needed:

1. There should be a regulatory requirement for them to do so, as long as they are given Criminal Codes that they can clearly link the report with.

Virus-free. www.avast.com

From:	Andrew Wade
To:	ICN / DCI (PCH)
Subject:	RE: the harmful online content legislation
Date:	August 26, 2021 12:30:41 AM

Hello,

This email is feedback in response to the current legislative and regulatory framework being considered: <u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html</u>

This legislation should not be passed. It will endanger the lives and livelihoods of Canadians while also curbing legal speech online. By issuing harsh penalties for underblocking (poorly defined) banned speech online, without any penalties for blocking legal speech online, companies will be incentivized to block everything that could possibly be seen as inappropriate. It also incentivizes inaccurate, algorithmic removal of content without repercussions.

These are bad ideas. Do not let them become law.

Cheers, Andrew Wade, a Canadian

 From:
 Manuela Kesseler

 To:
 ICN / DCI (PCH)

 Subject:
 Please stop censorship...and hate speech!

 Date:
 August 24, 2021 8:18:36 PM

 Attachments:
 ATT00001.txt

To Whom It May Concern,

First of all, I would like to thank you for allowing citizens to voice their opinions and be heard. Lately, it has started to feel more like we are saying goodbye to democracy and hello to dictatorship. I never thought or hoped I would live to see this day come.

and I love my job!

Among the things I teach my students, one is being careful to sift through "fake news". I believe this to be a very important skill for them to learn in their research. For all of us. Anything else is a bandaid and can be used and abused just as much.

I have spent a large part of my summer doing research on the vaccine and I am blown away by how many medical experts have been censored thus far!

Even a co-founder of one of the vacccines, for simply stating up front what he knows about the spike protein! It's factual stuff!!

I agree that platforms can be abused and it is sometimes hard to hear hate speech and people sharning. However, my concern is also this: who would choose this Advisory Board? And would it be made up of people with differing opinions or would they be hand-picked to move a certain agenda forward?

Bottom line: I am against censorship!

I believe people need to be properly educated in how to discern right from wrong and not take everything personally just because someone with a different opinion said something contradictory or offensive.

We need to hold fast to democracy. It is part of our country's makeup and the reason it is such an amazing place! Without it, we may as well be a Communist country. Surely that is not the goal?

As well, I would like to address this part of your website statement:

s.19(1)

From:	diol (Ne. ACCESS 10
To:	ICN / DCI (PCH)
Subject:	Have your say: The Government's proposed approach to address harmful content online
Date:	August 24, 2021 8:06:54 AM

Free speech is the foundation of democracy. Everyone wants to stop "harmful" content but the problem is what is "harmful" content and who gets to define it.

As with any problem there are no solutions only trade-offs. The worst trade-off with the proposed harmful content online rules are the restriction it imposes on free speech. It seems unfathomable to me to have the government control what it thinks is harmful. This is the slipper slop to one-party rule.

For example, the government could deem that criticism of it climate change policies are harmful content and not allow any alternative policies to be proposed.

This proposed approach to address harmful content online must not be allowed to be implemented. Daryl Olson

s.19(1)

From:	tom.stesco
To:	ICN / DCI (PCH)
Subject:	Comments on proposed approach to address harmful content online
Date:	August 24, 2021 12:28:55 AM

To whom it may concern,

The discussion we are having in Canada on what to do about harmful content on social media platforms is very important. The Government's proposed approach to address harmful content online as explained on <a href="https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html">https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html</a> and associated documents is far too broad and stifling to future online content.

Required 24 hour response times (or any time that in aggregate necessitaes automated censorship) removes all possibility for nuance online. Alot of online speech would be censored by default. Important discussions would be censored if popular and devisive enough, forcing further polarization of our society.

The technical implementation would require massive infrastructure changes that would effectively make Canada impossible or risky for many online businesses to operate and hire Canadian people or otherwise provide value to Canadians.

No matter your opinion of online content and it's darker examples, one must obviously see that the subjectivity in regulations as proposed would allow for future redefinition of harmful content and subsequent hardlined censorship of things not originally intended such as: politics, scientific research, whistle blowing, and open source software.

As a Canadian citizen who genuinely believes our Government is trying to do the correct thing I think we must do better to not inadvertently turn our online commons into a censored desert.

Yours truthfully, Thomas Stesco

From:	Jacqui Ehninger-Cuervo
To:	ICN / DCI (PCH)
Subject:	Bill C-36
Date:	August 23, 2021 4:08:03 PM

To Whom It May Concern:

I saw on your website (https://www.canada.ca/en/canadian-heritage/news/2021/07/creating-asafe-inclusive-and-open-online-environment.html) that you are seeking feedback about bill C-36, which is meant to limit on-line harm.

While this looks like a noble goal at first glance, it becomes apparent very quickly that this bill has no place in a functioning democracy that values free speech: The concepts of a secret complaints system, cash rewards for complainers, and the "Department of Pre-Crime" sound like they've been taken straight out of a dystopian novel!

We already have legislation to prevent hate and discrimination and that is a very good thing.

We do **NOT** need a bill that proposes to amend the criminal code so that every blogger, publisher, Facebook and Twitter user could face house arrest or large fines of up to \$70,000, if someone complains about them.

Moreover, if I read the proposal correctly, people would be considered GUILTY until proven innocent – not the other way around! When did that happen? Isn't it supposed to be innocent until proven guilty?

We have sufficient legislation in place to prevent hate and discrimination – Canadians do not need or want any additional internet censorship.

This bill is unacceptable and in conflict with our constitutional rights and freedoms.

Sincerely, Jacqueline Ehninger-Cuervo

From:	Jesse Betteridge
To:	ICN / DCI (PCH)
Subject:	Feedback: The Government's proposed approach to address harmful content online
Date:	August 23, 2021 2:54:53 PM
Date:	August 23, 2021 2:54:53 PM

While I believe that hate speech has become one of the biggest problems online and that Canadian laws are currently inadequate for holding the social media companies who allow it to proliferate accountable, I feel that the approach being proposed for tackling this problem is greatly flawed and requires major revision.

The government's approach should focus on holding specific social media giants, such as Facebook and Twitter, accountable for the hateful content that they allow to proliferate on their platforms and often fail to reign in. However, any actions that go beyond simply holding these platforms accountable falls outside the scope of what this approach should cover.

The current proposals fail to evaluate many of the strengths and weaknesses that have already been encountered by other countries who have made similar efforts. One particularly problematic element is the length of time for regulated entities to make offending material inaccessible after being reported: 24 hours. Most regions that have introduced or proposed similar measures have required 7 days. While even 7 days is arguably an unreasonably short period of time, it at least provides a reasonable opportunity for content to be properly evaluated. A 24 hour period will greatly increase the chances for social media companies to remove content in error with no opportunity for recourse. This is something that already happens with their existing systems, and it disproportionately impacts speech from the victims and marginalized groups these rules are intended to protect. With an impossibly short turnaround like 24 hours, this existing problem will almost certainly get worse.

The current proposals also introduce the possibility for social media companies to police "potentially" hateful content through algorithmic filters. Given the problems that already exist with the way these companies handle moderation, the potential negative impacts to victims and marginalized groups are increased even further. There need to be significant measures, if not outright penalties, for companies that erroneously remove content that is not harmful.

Creating an environment in which social media companies could potentially have to create significant data retention policies could also prevent smaller social media entities from operating in Canada, or even worse, create disincentive for new services to launch, ensuring that the current social media giants are the only ones who can operate. Significant considerations need to be made to ensure that this does not happen, and that the majority of these expectations are only applied to specific companies on a case-by-case basis. Even requiring a threshold of user base or net worth will not really work.

Perhaps the most problematic element of these proposals is the ability for a regulatory entity to block or take-down websites, which is significant overreach which could have a devastating impact for the free internet to properly function in this country. You must revise this aspect and create alternative disincentives for regulated sites.

Thank you for your consideration.

Sincerely,

Jesse Betteridge

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act.

From:	osearth The Access to Information I
To:	ICN / DCI (PCH)
Subject:	over reaching poorly planned &n agreement backpeddling standard being set by Canada - The PEACE-KEEPERS
Date:	August 21, 2021 10:36:10 PM

There needs to be an open 0nly public moderated debate on this matter. ALL ONLINE CANADIANS DESERVE IT especially our children WHO WILL BE PAYING THE TRUE PRICE FOR THIS CRIMINAL BACK RROM CIGAR DRENCHED DRAFT...

s.19(1)

From:	Levo DeLellis
To:	ICN / DCI (PCH)
Subject:	Harmful Online Content Proposal
Date:	August 21, 2021 10:17:24 PM

Hi I was reading this article <u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html</u>

I absolutely hate it. Especially the fact there's automation (which Module 1(B): 10 A leads me to believe) and reporting. I work in the software field and seen filtering and machine learning fail repeatably. There are other things in the proposal that seems extreme

I'd be ok with some of the following

- Warnings were added to suspicious content

- Advisories on strange groups such as flat eathers and anti vax. Perhaps a learn more link which informs users about "Russian troll farms" and that members of the group may not believe anything they're saying but intend to cause disruption in their lives

- Having social medias inform users how many hours they spend and suggest to take breaks

But nothing that prevents anyone from doing anything (it may stop a person from being able to contact another at a time of need). Nothing that mixes automation with reporting

An example of why you never impede is below. In the UK they activated a filter that wasn't opt in. It disrupted a large company and hundreds of thousands of players. https://www.gameskinny.com/w9kbu/league-of-legends-not-patching-uk-porn-filter-blocks-more-than-porn

From:	Kendra Floren
To:	ICN / DCI (PCH)
Subject:	Digital Citizen Initiative
Date:	August 21, 2021 7:28:10 PM

Canadian citizens categorically do not need or require any form of government body to monitor and decide what forms of expression, content, or media are permissible for their consumption on the internet. Any content that is not already a violation of the law should be free for all Canadians to access. Any sort of attempt to limit or control Canadian's access to legal content of their choosing, especially one has slapdash and overreaching as this one proposed, is a gross violation of Canadian's rights. Do not control or legislate our access to data on the grounds of some laughable standards of moralizing.

ne Access to	1
CH)	
ay: The Government's proposed approach to address harmful content online	
021 4:50:47 PM	
P	er PCH) ray: The Government's proposed approach to address harmful content online 2021 4:50:47 PM

Regarding

https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html

Over broad powers for inspection, country-wide website blocking, secret trials, huge penalties, regulatory charges to fund it all. These are all terrible ideas.

This is Canada, please try again.

Sincerely,

Robert Basler

s.19(1)

From:	Jonathan Wolframe-Smith
To:	ICN / DCI (PCH)
Subject:	The Government's proposed approach to address harmful content online
Date:	August 21, 2021 1:13:02 PM

Good afternoon,

I am writing as a concerned Canadian citizen with regard to the recent call to have my say on the government's proposed approach to address harmful content online.

s.19(1)

Having reviewed the proposed documentation, I ask the government pay due attention to the needs and concerns of self-identified sex workers during this process, such as those identified by the advocacy organization the Canadian Alliance for Sex Work Law Reform (https://sexworklawreform.com/). While I am not a sex worker myself,

I am proud to call myself an ally to and serve the needs of a variety of marginalized people, including sex workers, from a place of non-judgemental and autonomy-bolstering care.

I applaud and encourage the government's efforts to address the seemingly growing problem of hate speech and discrimination online. It is my hope that the government examination of this problem will involve careful and considered consultation with sex workers as stakeholders in their own autonomy and ability to make a living online as consenting workers, distinct from any valid concerns regarding non-consensual sexual abuse as it appears online.

Thank you very much for considering my concerns on this matter.

Sincerely,

Jonathan Wolframe-Smith

Patricia Gibson
ICN / DCI (PCH)
Demise of canada
August 21, 2021 12:15:04 PM

This country has fallen into the hands of the communist party of China ! Thanks to our Corrupted politicians across the board . All levels. Our health care system can no longer be trusted as they are forcing people to take a vaccine that has been through no clinical trials. What a disaster. Shame on the health care workers pushing this agenda on an uninformed brain washed public . Only the doctors and politicians who are risking their livelihood are to be believed .

The media are the top criminals after the politicians for being bought off on order to advance all this corruption. Canadians need a severe wake up call and a good history lesson .

Shame on all of you for ruining this what used to be a great country. Patricia Gibson

Sent from my iPhone

 From:
 Michael Suksi
 Met Address if

 To:
 ICN / DCI (PCH)

 Cc:
 Sven Spengemann

 Subject:
 Have your say: The Government's proposed approach to address harmful content online

 Date:
 August 21, 2021 11:18:27 AM

I am writing to comment on the proposed approach to address harmful content online. I have three comments to make.

First, I strongly support this initiative. I support it because I believe there is great harm being done online in the five categories that are addressed in this proposed approach. While I recognize the other side of the debate is the need for preservation of free speech, I strongly believe that the collective benefit of stopping/reducing the harm outweighs the collective benefit of free speech in these areas. Also, on a more detailed note, I assume **Bitchute** will be one of the media channels that is regulated? I don't see them listed in the discussion papers I've read.

There are two other areas of internet communication that are also causing harm and that do not appear to be addressed by this proposed legislation.

What about the need to truthful content? In addition to the five areas already identified, I believe there should be a sixth consideration, which is the need for truthful content. Of course, work would have to done on the specifics of how this is defined, but I'm in favour of an approach that legally defines an internet publisher's obligation to make reasonable efforts to ensure that content presented is factually truthful. For practical

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

purposes, perhaps this does not apply to individuals who Act are posting comments on social media because it may be too hard to monitor and enforce...I don't know. But, certainly larger content creators should be regulated in this way.

How do we regulate web sites that present news or political content, but are not considered to be "social media"? There are Canadian based web sites that are spreading misinformation and encouraging hatred online and they must also regulated. For example, in my opinion the Rebel News site is spreading false information and encouraging extremist right wing anger and even violence. I'm all for having a variety of opinions, but are web sites like Rebel News regulated the same way that other mainstream news outlets (i.e., CBC, Globe and Mail, Toronto Star, etc.) are regulated, and if not, what do we do about that?

Thank you.

Michael Suksi

s.19(1)

 From:
 Robert Leslie

 To:
 ICN / DCI (PCH)

 Subject:
 Censorship

 Date:
 August 21, 2021 9:33:40 AM

s.19(1)

Why do you want to do this? We already have hate laws. One is only left to wonder if you are just trying to stop any and all opposing views. That really is quite shameful. But then all of what you're doing is to bring down a once great country. Make Canada strong again. A proud Canadian. Marguerite Leslie

From:	catherine tracy (Inel ACCess TO )	
To:	ICN / DCI (PCH)	
Subject:	Having my say: The Government's proposed approach to address harmful content online	
Date:	August 21, 2021 7:29:58 AM	

## To whom it may concern,

This proposed law (intended to combat hate speech and other kinds of harmful content online) is extremely misguided and must not be passed. All it takes is for those in power to decide that legitimate criticism of themselves counts as "harmful content" and our democracy will be in real peril. This sort of law is proposed when people naively think that those in power are always going to be decent, thoughtful people, but it will also give extraordinary powers to dangerous power-hungry people that manage to get elected.

Please do not pursue this proposed legislation.

- Catherine

Dr Catherine Tracy, Dept. of Classics, Bishop's University, x.2877

Steve
ICN / DCI (PCH)
Censurer au profit de qui?
August 20, 2021 8:53:47 PM

Avant les années 2000, la télévision analogique était gratuite et arrivait par l'antenne. Puis, on nous a vanté la télé numérique de meilleure qualité, qui permettait en même temps une meilleure utilisation du spectre de radiodiffusion. Peu de temps après la télé gratuite à disparue, et les compagnies de diffusion se sont mis à encrypter les canaux qu'on avait gratuitement, pour nous les faire payer.

L'encryption que vous vouler interdire à Pierre, Jean, Jacques, vous le permettez à Shaw direct, Bell, Vidéotron, etc. afin qu'ils puissent nous priver d'un service qu'on avait gratuitement jadis.

#### Vous centralizez!

Vous dites vouloir légiférer les géants du Web tels que Facebook et Netflix, mais vous en êtes devenu dépendant. Le seul moyen pour que votre contrôle de l'internet fonctionne est justement que tout le monde adhère à ce Facebook et ce Netflix. Si les gens utilisaient des plateformes décentralisées, vous auriez du mal à appliquer vos méthodes de contrôle.

Vous misez sur la centralisation. Vous essayer d'avoir votre part des monopoles. Quelle honte! Nous sommes un peuple guidé par des dirigeants soumis! Pire, vous allez mettre des bâtons dans les roues à ceux qui s'éloignent des sentiers battus.

s.19(1)

 From:
 Dan Berry

 To:
 ICN / DCI (PCH)

 Subject:
 Restrictions

 Date:
 August 20, 2021 8:41:55 PM

Dan berry

 From:
 Lisa Agozzino

 To:
 ICN / DCI (PCH)

 Subject:
 No to C-10

 Date:
 August 20, 2021 1:42:18 PM

Good day,

With regards to bill C-10. This will cost taxpayers more money.

The funds should be going to fertility. Our fertility rates are dropping..... If our fertility does not increase, who will you police over the internet?

Please allocate our tax payer money in another way.Send us a questionnaire to each of our cell phones to vote on this. It is not your decision to take. Fertility treatments are 15 000\$ for one in vitro try.

People will only access the black market for content. This is like the war on druge. Waste of time and money.

make us vote on this. Send us each a text message or email.

Thank you.

Lisa



Virus-free. www.avast.com

 From:
 D.R

 To:
 ICN / DCI (PCH)

 Subject:
 Slippery Slope

 Date:
 August 20, 2021 8:43:57 AM

# Good Morning

I had tried to read the document, it seems to me that once this has been passed the government will be able to make privacy decisions and changes without actually putting it before the people.

This is Dangerous, I also think that it will just force those who are using these unmonitored services now even farther underground, Which means our law enforcement will have to dig even deeper to find them.

Just my opinion but I am seriously worried about the trend today to curtail freedoms because of some bad actors. There has to be a different way of doing this. passing a law is not always the answer.

Have a great Day

**Dennis Reuel** 

"Not everything that counts can be counted and not everything that can be counted , counts " Albert Einstein

1

Virus-free. www.avg.com

s.19(1)

From:	the Access to Information	
To:	ICN / DCI (PCH)	
Subject:	Re: Have your say: The Government's proposed approach to address harmful content online	
Date:	August 19, 2021 10:47:15 PM	

Dear members of the Department of Canadian Heritage,

My name is Christian Fielding, and I am the owner/administrator of a very small online wiki with an integrated forum, and users are required to make an account, which in turn has to be approved by me before they can contribute anything to the site.

I am pleased that the government of Canada is taking steps to combat online harms, however, I do have a few concerns about the implications of these proposed regulations on small platforms, like mine.

One notable concern is the fact that automated systems for detecting harmful content are simply inaccessible to small platforms. Many of these systems are very costly, or are given out for free, but only to large tech companies. I am relieved, however, that the proposal says that platforms must take all reasonable measures, which can include automated systems (implying that they won't be mandatory). If these automated systems are mandatory, one option could be that they would only be made mandatory for platforms that wouldn't be able to reasonably regulate themselves without them (such as major platforms). Many major platforms already use such systems. In my case, where my site is a wiki/forum with only a few members, I am easily able to monitor the entire site (Thankfully, there have been no instances of any type of harmful content present on my site). In my case, simply having myself monitor the site for harmful content is a reasonable approach for a site of this size. If it ever grows larger in the future (unlikely), then automated systems will have to be considered by me. Another concern with automated systems as a whole is they usually lack the ability to determine context. There have been instances where videos discussing the horrors of Nazi Germany and the Holocaust have been taken down for "inciting and glorifying violence", when the exact opposite was true. These types of situations should be taken into account before any such systems are implemented or mandated.

Another concern is the funding of the regulators by the regulated platforms. My site is a personal endeavour, does not run ads, or make any type of profits or revenue. It would simply be impossible for me to pay regulatory dues, due to the fact that my site does not bring in any money, and in fact, costs me money (domains and hosting). One option (which has been proposed in various section 230 reform bills from the U.S.) is that these financial obligations would only apply to platforms with a certain amount of active monthly users, or revenue. Another option is to only apply these financial obligations on for-profit. These solutions could also apply to the automated filter issue.

I would like to thank you for reading my email, and hope you take these recommendations into consideration.

**Christian Fielding** 

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to tion ACL

From:	Loeska Guenther
To:	ICN / DCI (PCH)
Subject:	bill C36
Date:	August 19, 2021 4:26:48 PM

## Hello,

I am deeply concerned with this proposed bill. The unintended consequences of similar legislation in other countries has included the further maginalization of protected groups, loss of livelihood for women and sex workers and the destruction of educational and supportive online spaces by tech companies being overly cautious in their application of laws/regulations.

SImilar legislation has been struck down in the French courts because it clearly violates the human rights that are intrinsic to a democratic society.

This proposed legislation is extremely dangerous and at best will waste millions in tax payer money in court challenges and at worst will result in the destruction of free and open communication and the deaths of marginalized people whose support systems and incomes will be destroyed.

The government of Canada has a duty to protect the human rights and well being of Canadians. This proposed legislation does the opposite and if implemented will directly contribute to harming individuals and undermining our democracy. It must be completely scrapped. This type of legislation has proven to be ineffective at dealing with the issues it attempts to address and has instead made predators and abusers even more difficult to track. FOSTA/SESTA in the US has driven traffickers even further underground where law enforcement cannot find them.

Hopefully with the snap election this proposed bill will die on the table but if not it must be abandoned and replaced with an entirely new framework built in consultation with both experts in internet socioeconomics and the Canadian public.

Thank you. Loeska Guenther

 From:
 Ian McIntosh

 To:
 ICN / DCI (PCH)

 Cc:
 MP Salma Zahld

 Subject:
 Online Lies

 Date:
 August 19, 2021 12:54:46 PM

Another type of harmful online content is lies; for example, untruths about Covid-19 and the vaccines for it. These lies are causing deaths, and something must be done to remove them and to stop and in many cases prosecute their sources and spreaders, and to make social media enabling them remove and prevent them.

- Ian McIntosh

s.19(1)

 From:
 Mark Purkis

 To:
 ICN / DCI (PCH)

 Subject:
 Bad Idea

 Date:
 August 18, 2021 9:16:24 PM

This is such a terribly thought out, terribly rolled out, and terribly exploitable policy.

Please refer to the many more articulate and expert voices in this inbox, but do count my voice of opposition to the currently proposed "harmful content" internet regulation(s).

Mark Purkis

 From:
 J. Lucas Donkers

 To:
 ICN / DCI (PCH)

 Subject:
 Your Harmful Online Content Proposal

 Date:
 August 18, 2021 6:19:53 PM

I'm writing in regards to the Harmful Online Content proposal at: https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html.

I have read the discussion guide at

https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html, and find it poorly written and broadly worded.

You are asking for "regulated entities" to provide reasonable measures to make harmful content inaccessible in Canada, but what is are "regulated entities"? Who's to say exactly who or what falls into that category? You are asking for 24 hours from the time a user flags any content they deem harmful, or indeed anything they don't like for any reason. The regulated entity then must decide based on their own algorithms which they have to \*try\* to fit your rules. 24 hours means that this has to be automated because it's impossible for any company to have a human view the content and make a decision. This means that content will be taken down whether or not the algorithms have accurately identified the harmful content. So, you have no absolute definition of what "regulated entities are", no human interaction, no control over how the algorithms actually work, and anyone can game the system by flagging anything they want as harmful content.

You are also asking for Internet Service Providers (ISP) to somehow monitor for child abuse material, and provide evidence and personal information pertaining to the possible offender. But don't say how to actually do this, and you may not be be aware that most information is now encrypted during transit by default, and ISPs can't view the decrypted information. And, once CSIS receives all these notifications of possible violations of the code, based on whatever algorithms they write to try to comply with your rules, what happens then? Are all those people raided by the RCMP, arrested, their lives torn apart before the RCMP discover it was just a mistake? I see nothing spelled out about how this is supposed to be accomplished without violating every Canadian citizen's fundamental rights. You are making ISPs responsible for everything their users say and do. Last I checked, nobody holds Bell Canada accountable for their customer's speech over telephone.

In summary, you are writing laws that will very likely destroy people's lives on the whim of an algorithm you have no control over. You are making "regulated entities" and ISPs responsible for their customer's words and content. You are also taking away people's right to free speech, and people's ability to decide what content they want to view.

Please give careful consideration to how this will actually be used, how it will work, don't make company's responsible for the words of their users, and tighten up the wording of your proposal, so that there isn't any interpretation of the law.

Regards,

Justin Donkers s.19(1)

From:	Aron Rosenberg
To:	ICN / DCI (PCH)
Subject:	Feedback on the Government's proposed approach to address harmful content online
Date:	August 18, 2021 3:08:33 PM

Dear Digital Citizen Initiative Committee,

My name is Aron Rosenberg and am researching the internet and how young people can be more responsible and critical online.

My research is focused on creating safer and more equitable digital spaces and I am therefore very concerned about this new, proposed legislation. It will make it harder for smaller tech companies to exist (due to the financial costs of the kinds of censorship suggested by the new regulations), thereby allowing larger tech companies to maintain a monopolistic share of the market. This is particularly concerning for youth because young people have NOT historically been protected or served by these large tech companies. The proposed regulation would also promote a sweeping, fast-paced kind of censorship that is likely to accidentally censor legal, acceptable content: such as safe forums for sex workers, discussions about contentious political issues, and satire. As a democratic country, it is important to ensure careful, transparent processes are used to censor speech and this new legislation is proposing to do away with a lot of the slow, transparent processes that already exist to police harassment and hate online.

I would be more than happy to discuss this further. It may even be interesting to get some high school students involved in this conversation. Please be in touch if you'd like my support facilitating youth focus groups on this. I can be reached here by email or by phone at

Thank you for reading my feedback, Aron Rosenberg s.19(1)

Katheryn Saelens	Ņ
ICN / DCI (PCH)	
RE: The proposed approach to address harmful content online	
August 18, 2021 1:00:38 PM	
	ICN / DCI (PCH) RE: The proposed approach to address harmful content online

Yeah, I am all for banning online content that has to do with child sexual exploitation content (LIKE ON FACEBOOK!), terrorist content, content that incites extreme violence, and the non-consensual sharing of intimate images...these are no-brainers. However, banning hate speech AKA: "words that hurt" is ridiculous because this is a FINE LINE and is up for some serious interpretation that I do not think the government is capable of determining AT ALL. Even Facebook has tried to determine it because it can't handle criticism whatsoever and has failed miserably overall.

There will always be "hate" online and that's just part of FREE SPEECH and I wouldn't try and take any of that away from Canadian citizens or you are going to have A LOT of angry people that will be pushing back at this nonsense. Stop trying to turn Canada into a communist regime, it's getting really noticeable and won't be tolerated.

NO ONE here in Canada, with half a brain wants this unless they can't handle harsh words and are unable to UNPLUG and get off the internet. Truly, that is their problem and as far as politicians not being able to handle harsh criticism online, well again they need to put their big boy/girl panties on stop crying about it because harsh criticism goes with the territory.

It's actually laughable that this subject is even being broached in the first place.

Simple as that.

- K. Saelens

From:	Gav Sarafian (he Acces	
To:	ICN / DCI (PCH)	
Subject:	Feedback: Government's Proposed Approach to Address Harmful Content Online	
Date:	August 18, 2021 10:50:02 AM	

#### Hello,

As a Canadian citizen, I am deeply concerned by the government's proposed approach to address harmful content online (as described here: <u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html</u>). The proposed changes seem to adopt the absolute worst parts of similar laws adopted by other countries (in particular, the USA's SESTA/FOSTA bills), while completely ignoring the harmful effect these laws have had.

The proposed changes will affect our ability to express ourselves freely online. While the goal of the bill makes sense, the means will result in a mass silencing that will affect marginalized people the most. Requiring making content inaccessible 24 hours after being flagged will result in companies removing content simply because it was flagged - which often are false negatives, severely impacting the average internet user's ability to express themselves. How can we rely on this to protect ourselves? All but the largest companies will simply choose to censor their users, regardless of the validity of their content.

In Canada, we have decriminalized sex work. However, making a living as a sex worker is still prohibitive, especially when it comes to screening clients. Speaking as an outsider to this industry (but have many friends who work in it), safety is paramount. After SESTA/FOSTA passed in the US, we saw a rapid shuttering of many sites that were seen as safe places for sex workers to share information, especially that which they could use to keep each other safe (ie; not only to source clients, but to share which ones were 'bad dates'). These bills also had a chilling effect on LGBTQ2S+ people online, as it has become harder to share information without some of it being flagged as 'inappropriate'. I see the currently proposed changes to take on only the worst of other, similar changes elsewhere in the world, with nothing to ensure its actual goals are met. Nobody has been made safer because of these changes.

I implore our government to drop this proposal, and go back to the drawing board. As a citizen who grew up alongside the developing internet, it feels like these proposals were written by persons with either limited knowledge of how the internet functions, our basic freedoms, as well as the dire ramifications for marginalized peoples across the internet.

Thank you, Gav Sarafian

 From:
 Debra Wilson

 To:
 ICN / DCI (PCH)

 Subject:
 On line censorship

 Date:
 August 17, 2021 3:27:55 PM

Online censorship for matters that are contrary to gov and media narrative IS unconstitutional!

Kill all bills related to this type of censorship.

Good afternoon,

Thank you for the opportunity to express our comments about the "new" approach to address harmful content online.

This is what itos been stated:

"The Government of Canada is committed to taking meaningful action to combat hate speech and other kinds of harmful content online, including child sexual exploitation content, terrorist content, content that incites violence, and the non-consensual sharing of intimate images. The Government is asking for written submissions from Canadians on its proposed approach to make social media platforms and other online communications services more accountable and more transparent when it comes to combating harmful content online."

While I completely support the combat of harmful speech – not only in social media but in life, this proposal here is actually censoring some voices to speak. We have to PROMOTE good values and measures to ensure Canada remains as a free and safe country. Censoring and "regulating" even when the goal seems noble, is still censoring and regulating...like some communist countries do.

Is Canada walking towards regulating of media and speech? That sounds scary, whatever the reason is. I would not like to live in a country like that.

Thank you again. Sincerely

Myriam

Jim McIntosh
ICN / DCI (PCH)
Government"s proposed approach to address harmful content online
August 17, 2021 12:47:45 PM

What is the purpose of such a proposal?

- Is it to make up for deficiencies in the current criminal code that make it difficult to investigate and prosecute existing crimes? OR
- 2. Is it to create a whole new set of 'crimes' under the term "Harm" which will include concepts which do not include physical harm?

If the former, the better solution is to amend the existing legislation to remove the deficiencies. If the latter, I would ask why the force of law is required to prevent 'harm' which is not already criminal. Given it is aimed at ideas presented on the Internet, it appears to be an attempt to limit free speech, which is one of our fundamental freedoms protected by the Canadian Constitution. If you proceed to implement these ideas, I have no doubt it will cost me and other taxpayers thousands of dollars in court costs and legal fees, in addition to the costs of the bureaucracies required by the legislation.

Please do not infringe upon our freedom of speech, unless you intend to destroy democracy (or is that 'harmful').

Regards - Jim

"Any society that would give up a little liberty to gain a little security will deserve neither and lose both" - Benjamin Franklin

From:	the Access to In
To:	ICN / DCI (PCH)
Subject:	Have your say: The Government's proposed approach to address harmful content online
Date:	August 17, 2021 11:52:49 AM

I just wanted to caution against limiting or restricting freedom of speech.

I just noticed in the workplace how essential it is to have people who think orthogonally. Everyone who thinks the same will never think of alternate solutions which leads to bad outcomes.

Someone who thinks orthogonally comes in, expresses an alternate viewpoint and it challenges everyone to rethink their assumptions.

This is essential for development. For the progress of society, some discomfort and discourse is essential, otherwise we go into restrictive thinking and repressiveness.

A coworker once mentioned to me how he does not trust studies from certain countries, because, in his words, "concern comes from personal experience with scientists from China. They tend to manipulate the truth, especially the ones who have ties to the government. I have also found this to be the case with other nationalities that do not promote individualism"

I even heard of a study in which young people were more depressed because they were associating with those who only agreed with them and their viewpoint. It seems counter-intuitive, but oddly enough, is probably true. It seems to make an emotionally weak society.

It is important to guard that any law implemented cannot be extended or used in the wrong way, or manipulated to someone's bad intent.

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act.

From:	Blaine Pauling
To:	ICN / DCI (PCH)
Subject:	Addressing harmful content online
Date:	August 16, 2021 3:06:17 PM

Hello

I have serious concerns about the government of Canada's planned legislation to address harmful content online.

You have no doubt heard similar concerns from more articulate parties than me, so I will restrict my response to a few points:

1) algorithms run a high risk of misidentifying prohibited expressions

 the large penalties for non-compliance ensure that platforms will err on the side of caution and apply a wide net, blocking perfectly legitimate expressions

 how can a framework possibly outline what is harmful and reliably cover everything without over- or -under teaching

 this attempts to create a gatekeeper for acceptable expression - which is almost certainly going to reflect an ideological agenda

5) enormous risk a later government (of the same or a different party) will use the legislation to enact even more problematic, or potentially highly dangerous ideological constraints - left or right wing - t is imperative that the government not create mechanisms that could be easily abused by a future government

Regards Blaine Pauling

 From:
 JL

 To:
 ICN / DCI (PCH)

 Date:
 August 16, 2021 1:23:06 AM

Do not pass this. The government is not a "babysitter". People can decide who they wish to interact with online. One person's freedom to express criticism or potentially "offensive" thoughts with others, should not be taken away by unconstitutional overreaching rules in place by government. These measures have failed to improve society in other countries, and should not be implemented in "Strong and Free" Canada.

From:	Pale Greenwood
To:	ICN / DCI (PCH)
Subject:	Proposed Internet Censorship / Safety Laws
Date:	August 15, 2021 11:16:06 PM

To whom it may concern,

Forgive me for not knowing the name of the bill yet, but I'm writing in from BC over this proposal (

https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html) and I just want to say that 1) I hate it, and 2) it sucks.

With the tl;dr out of the way, please forward this off to whoever needs to actually hear it. I am not mad at whoever has to sort through the emails, I am mad at whoever actually thought this was a good idea, and I want my ire to be directed towards and heard by them. That being said:

Firstly, you are aware that Canada is not the only country to use the internet? And secondly, you are aware that all this is going to do is make things more difficult for marginalized communities, allow shareholders of VPN services to make more money than you, and gut anyone's interest in working with the internet in this country? I don't mean to imply the person who wrote this proposal is an idiot and doesn't know how the internet works, but of course I mean that, because we have been through this rodeo and it ends the same way every single time.

Face it: when you make something illegal, particularly in the realm of free speech and knowledge, you also make it illegal to argue against it. You can't say "Look, here's all the racist things I've gotten in my email," if depicting racism is illegal. Now, we already have hate speech laws against directed, targeted hate speech; and that does its job pretty okay. But keep it to that. Someone depicting racism isn't always doing it to be racist, and no matter how you write those laws, I want you to ask yourself "And if someone with opposite morals to me has the power to enforce this law, what will happen?" and you better write that law so they can't weaponize it against people like you.

I've been in plenty of communities and scenes where they said "no racism" and you know what happened, half the time? The Black person couldn't talk about their experiences with being the target of utter hatred, but the racist white person could make horrific caricatures and make that Black person feel incredibly unsafe, and get away with it. Because you could DO racist things, you just couldn't SAY them.

And you want me to accept that on a national level?

Did you learn anything from America doing FOSTA/SESTA? How it did a total of - and forgive my French - jack or shit to actually prevent trafficking and child abuse, but it all but annihilated adult content and spaces? Now, I get it, you probably think that's a good thing because uh, "hurr durr porn sinful" or something, but not everyone lives by your rules. I draw the line personally at knowingly hurting others or doing irreversible harm to oneself. If people want to make dumb choices they can walk away from, let them. Freedom and all that.

Your censorship proposal sucks. It asks internet providers to do it, and they won't, they'll put in a filter that doesn't work and they won't care, and nobody will be any safer. This is

# Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

performative on your end and theirs, and you should feel bad. This will do NOTHING but for Act annoy the hell out of everyone at best and make everyone use a VPN and not invest in Canadian infrastructure, because of your asinine, draconian laws.

Rework it into something that has concrete data behind it, an actual plan on how to implement it, and can't be abused by people taking the easy way out (which they will. These are corporations. They'd rather go cheap than effective, every time, and if you're not accounting for that, you might need to change career, dude). And then we can talk.

I agree our current system isn't the greatest we could have. But you get nowhere by actively making it worse. So here's one complaint about it. I hope there's many more, and you do better next time.

Cheers, Pale (he/him)

 From:
 Benn Kimmis

 To:
 ICN / DCI (PCH)

 Subject:
 Harmful Content Regulation (I am 100% against it)

 Date:
 August 15, 2021 5:14:22 PM

#### Hi there,

#### s.19(1)

My name is Benn Kimmis. Canadian Citizen and am very concerned about your new proposal to regulate content online. Our country has a lot of problems, especially ones that affect younger generations such as mine. To list some: Rising costs of housing, Canada's lack of ability to attract more high quality jobs, etc.

Instead of tackling those issues which are extremely important AND time sensitive you're going to try and tackle something that isn't a problem. The internet is about the open and free exchange of ideas, and you want to stifle people with your new Orwellian legislation. The idea that we need an 'internet czar' who oversees what can and can't be said on the internet is ludicrous. Yes, words can hurt people but having a 'one-size-fits-all' block of certain kinds of speech isn't going to solve anything. The attempt of trying to monitor 30 million people online is also never going to work shouldn't even be attempted.

If someone is threatening violence against a group of people, that is an issue and they need to be investigated by police or special forces, but that is literally the **only** time we should be policing the internet. Otherwise we should not be spending any police time or budget investigating people for what they say online. Our police need to be out in the streets preventing violent crime not sitting behind computers waiting for someone to use a word they don't like.

I 100% will vote against whichever party brings this bill to fruition, and I will never vote for them again. Right now Canada is one of the most free countries in the world, and that is one of the things I love about it. Please don't go through with this unneeded legislation or I'm voting you out.

Thanks,

Benn Kimmis

 From:
 G/C McFadden

 To:
 ICN / DCI (PCH)

 Subject:
 "online harms" censorship of the internet

 Date:
 August 15, 2021 2:01:11 PM

I am appalled at the government's attempt to regulate "nice" behavior on the internet. There is a problem, their definition of "not nice" is vague and subjective. We already have a regulation regarding hate speech. The implementation of an appointed, probably unnamed Czar, with unidentified complainants and no legal recourse brings forward the problem found with the almost universally despised human rights commission. This is a move to allow those in power to stifle dissent and control any information they did not like. It is the type of regulation which leads to despots found in easten Europe. This is bad legislation and not compatible with free speech of a democracy. Gordon McFadden

From:	David Briggs MELAD
To:	ICN / DCI (PCH)
Subject:	Re: The Government's proposed approach to address harmful content online
Date:	August 15, 2021 12:19:24 PM

I think this proposal should be changed significantly in the following areas:

- Blocking websites has zero place in a free country. These tools will be abused in the future by less scrupulous governments.

- Stricter definitions on two categories of the five: Hate Speech and Terrorist Content. It will be useful for future, more authoritarian governments to conceptually stretch either of these.

- Wherever possible, allow the courts to deal with complaints / charges over the various tribunals.

- The limits for reporting complaints shouldn't be set by a Governor in Council. A committee or actual act of legislation should establish these boundaries for each category. There's too much potential for abuse here (e.g. future civil rights groups protests becoming "terrorism"; anything that could impact the status quo).

- This proposal aims to regulate organizations outside of Canada. The addition of new rules to follow will make it more difficult for smaller entities to provide content to Canadians. This further the moat of the large internet companies as they have the resources to handle this. Canadian citizens will experience more geo-blocking, and there's already a lot of that.

In general this bill affords the Government too many additional powers, and can be abused by future governments. "Terrorism" has been used to justify all sorts of terrible privacy eroding laws and surveillance regimes. The term is going to be stretched until it allows for tyranny.

**David Briggs** 

s.19(1)

 From:
 Ocanada Standinguard

 To:
 ICN / DCI (PCH)

 Subject:
 Free speech

 Date:
 August 15, 2021 12:04:37 PM

The Canadian government must NOT censor speech in Canada nor support it elsewhere in any manner.

From:	Jordan Cromble
To:	ICN / DCI (PCH)
Subject:	I do not support this new Internet Regulation
Date:	August 15, 2021 4:20:04 AM

It is an affront to both the spirit of the Internet and the Charter of Rights and Freedoms. Yet another piece of legislation conceived by individuals lacking the technical understanding of the medium, creating unenforceable controls that can not hope to address the challenges the legislation proports to tackle.

If the Liberal Government chooses to continue on this ill conceived course of action, this legislation will serve as the epitaph for my support and membership of the party. The only things liberal about this legislation is the amount of alcohol that must have been consumed to consider this a piece of workable legislation. Matched only by the hubris of its authors and sponsors.

Please reconsider this legislation, and meditate on the lessions of Bill C-10. This strategy smacks of Harper or Ford style Conservative ideology, and will mark the end of the liberal party as a viable choice for anyone less the 45 years old...

Please stop.

Jordan Crombie

s.19(1)

From:	dudeofea
To:	ICN / DCI (PCH)
Subject:	Feedback on "harmful content" proposal
Date:	August 15, 2021 1:46:52 AM

#### Hi,

I am corresponding to indicate my disapproval with some parts of the "harmful content" proposal (found here: <u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html</u>)

Specifically, of the 5 types of harmful content mentioned (terrorism, inciting violence, hate speech, non-consentual image sharing, child sexual content) I only disagree with the "hate speech" type which is not only unenforceable in my opinion, but also not conducive to a fair democracy. Let me explain:

The unenforceability should be obvious as even by your own admission "Removal alone may push public threat actors beyond the visibility of law enforcement and CSIS, to encrypted websites and platforms with more extremist and unmoderated harmful content". Outlawing VPNs will also not work as individuals can simply use the Tor Browser, coffee shops, work internet, ad-hoc mesh-wifi networks, starlink, etc. The more pressure is put to find an alternative, the more it will be sought out and implemented. If Cuba cannot stop free access to the internet, neither can you.

What's more, a 24 hour notice is far too quick to take anything down and with steep penalties such as the proposed 10 million dollar / 3%, it would seem to me that many internet companies will simply stop catering to Canada entirely. Since the idea of the proposal seems to be to shut out only the worst internet users, if many popular but not quite ubiquitous sites (so not youtube, facebook, etc) leave canada then that would create an even larger group of people whose mission it is to subvert this law, thus rendering it moot for all.

On to my second point, as I understand it hate speech can be content which is provably true but still hurtful to someone. I see many issues with this: how old must the offendee be to have it count as hate speech? Must the offendee belong to a protected group? Is it the subjective \*opinion\* of the offendee which determines the offense, or the subjective \*opinion\* of a human rights tribunal?

This echoes to me a sentiment many Canadians had with Steven Harper's "barbaric cultural practices hotline" (<u>https://www.cbc.ca/news/politics/canada-election-2015-barbaric-cultural-practices-law-1.3254118</u>). It seems to me this proposal wants to protect Canadian values as well, and if a conservative government takes the lead again, this proposal could be used for those means.

I believe a government should represent its people, which means that if 1% of Canadians are bigots and racists, then 1% of the government should be bigots and racists as well as 1% of the (Canadian) internet. We do ourselves no favors by attempting to hide the skeletons in our closet. If the government does not represent its people, then it is not their government, much like the failed attempt at the US to enforce its government on the people of Afghanistan. I

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

imagine there are many things which would be considered "harmful content" to an Afghani to n Act which the US would disagree, and vice versa.

Thank you for your time in reading this. -Denis

Peter Briggs
ICN / DCI (PCH)
Proposed legislation
August 14, 2021 8:47:04 PM

Censorship is censorship... rules as draconian as those being proposed will inevitably result in the opposite effect from their intention. It will drive truly radical and dangerous people even further underground, while infringing on the right of free expression for people evenly slightly out of the mainstream "norms" approved by government. It's an exceedingly dangerous precedent for the government-of-the-day to set limits on what is "acceptable" speech. This is wrong, flat-out wrong and Orwellian in the extreme. This must not pass, or our days as a free society are indeed numbered.

Regards, Peter Briggs

Sent from my Bell Samsung device over Canada's largest network.

 From:
 Deb

 To:
 ICN / DCI (PCH); Matt Giuca

 Subject:
 Proposal for harmful online speech control

 Date:
 August 14, 2021 8:23:30 PM

I'd like to lodge my complaint about the far over-reach of this proposed legislation. It goes far too far over the deep end into police state territory. The controls this government proposes will make it impossible for regular businesses to comply with any sense of timeliness to valid complaints. Not only will so-called harmful speech be removed but that unjustly removed will not be reinstated or re-evaluated. This is a draconian approach that goes much too far.

Deborah Johnson

From:	Glen H
To:	ICN / DCI (PCH)
Subject:	Harmful content feedback
Date:	August 14, 2021 8:18:21 PM

These laws you are proposing will make Canada less free. I don't want the government filtering things like China. If it is illegal then act. Don't make new laws about what you can't say on the internet. Let people speak and share their thoughts freely. If they do some thing illegal then punish them. Let speech be free so we can live freely, even if we don't like what someone else says.

Glen

 From:
 Jack Clarke

 To:
 ICN / DCI (PCH)

 Subject:
 Concerns About Digital Censorship

 Date:
 August 14, 2021 7:07:54 PM

Dear Digital Citizen Initiative,

I've recently read cory doctorows blog post about the proposed rules and believe that these rules are incredibly harmful for all canadians. Please do not let this bill become law.

https://pluralistic.net/2021/08/11/the-canada-variant/#no-canada

Thanks

Jack Clarke

 From:
 Ben Perkins

 To:
 ICN / DCI (PCH)

 Subject:
 C-36

 Date:
 August 14, 2021 6:56:24 PM

Whatever team dreamed this and C-10 up needs to give their head a shake. This isn't your mandate. People don't want this to happen, it can't be properly enforced and it hasn't worked anywhere else. Not a good luck heading into an election.

Mark Thomson
ICN / DCI (PCH)
proposed internet legislation
August 14, 2021 6:44:58 PM

I have reviewed the proposed legislation and agree with Prof. Michael Geist. https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/

This legislation is draconian and dangerous. It's dangerous to the freedoms we Canadians enjoy and dangerous to the internet-based economy in Canada. It will make us a global laughingstock and force innovation to move overseas.

The internet has allowed me to educate myself and generate a decent living wage. In my opinion, it is the greatest invention of the past half century. Locking it up with big-brother nanny-state legislation will active harm Canadians, our economy, and indeed, free speech *globally*; We should be looked to among our global peers as a shining example of freedom. Instead, this legislation brings us closer to Chinese style authoritarianism.

Mark Thomson

s.19(1)

From: To: Subject: Date: Alex Kursell ICN / DCI (PCH) Opposition to "The Government's proposed approach to address harmful content online" August 14, 2021 5:07:14 PM

Hello. I recently came across "The Government's proposed approach to address harmful content online", as seen at https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html. As both a Canadian citizen, and a someone currently enrolled in a university software engineering program, who has previously worked in the industry, I strongly oppose the proposal.

Specifically, I oppose it for the following reasons:

1. The proposal requires that "an OCSP must take all reasonable measures, which can include the use of automated systems, to identify harmful content". In other words, it requires not just that providers comply with regulatory orders to sensor speech, but that they preemptively create systems to enforce such censorship themselves. This has the following problems:

a. To avoid penalties, it is likely that companies would choose to make such systems even more strict than what the government requires, erring on the side of caution. Even if the government does not abuse its' power to censor speech, it is possible that these automated systems \*will\* end up censoring benign speech. As an example, speech inciting violence against Indigenous people is obviously harmful and is already illegal. An over-cautious automated system might instead choose to censor any speech relating to Indigenous issues \*at all\*. Note that in the context of machine learning (ML) systems, which would likely be used by large companies to comply with this requirement, this kind of over-zealousness might be "trained-in" to the system without any human ever explicitly trying to do so. While the proposal does require that these systems "do not result in differential treatment of any group based on a prohibited ground of discrimination", in practice this is almost impossible. Any system that has to classify something as vague as hate speech or violent content, will necessarily have false positives, classifying benign speech as problematic.

b. The requirement that OCSPs implement such systems tilts the field even more heavily in favor of technology giants like Facebook or Twitter. Having previously worked at Facebook, I can assure you that they have the resources to implement whatever system or processes that are required of them. Smaller providers, including niche web-forums or blogs, or providers funded by user donations, do not. The end result of this proposal will be the further centralization of discourse on the few already-large platforms with the ability and resources to comply with it. I should point out, in addition, that these smaller providers are often havens for marginalized communities, including, as an example, sex workers, or those with divergent political views (and I am \*not\* referring here solely to the far-right).

2. The proposal essentially moves from a "default-allow" to a "default-deny" stance on speech. As it stands now, anyone can initially

publish speech without restriction. If the government determines that this speech violates Canadian law, it can begin criminal proceedings. As far as I can tell, provincial human rights tribunals seem to operate in essentially the same way, with speech only censored and fines levied only after the speech is made, and subsequently determined by the tribunal to be against some human rights code. This proposal, especially considering the requirement for OCSPs to preemptively block possible harmful speech, reverses this. Instead, this proposal creates a "Digital Recourse Council of Canada" which instead only processes \*appeals\* for decisions already made by an OCSP to block content in order to satisfy regulators. Instead of some kind of process being followed in order to have speech be censored, speech can instead be censored arbitrarily by OCSPs in order to comply with this proposal, with people then having to contest these decisions in order to have their speech allowed.

I have become increasingly worried about my government's apparent disregard for free expression and free speech, especially as practiced over the internet. Bill C-10

(https://parl.ca/DocumentViewer/en/43-2/bill/C-10/third-reading) drew heavy criticism for similar reasons as this proposal, as it was unclear whether that Bill would require the CRTC to regulate user-generated content. This proposal \*explicitly\* requires such regulation.

While I recognize that child pornography and hate speech are real concerns and that they do real harm, this proposal has the potential to do massive harm as well, by essentially creating a framework by which the government and large tech corporations have the power to preemptively censor any speech without any more due process than the decision of an automated filter. This will have a chilling effect on public discourse as a whole, even if the actual scope of what is subject to censorship is limited to what is already illegal under Canadian law.

Public discourse is essential to the operation of a free society. As Canadians, we recognize that there are some limits to that discourse where speech has the potential to violate the human rights of others. But there is a world of difference between giving the government the ability to, in limited cases, prosecute people for harmful speech in court, and creating a massive censorship regime, enforced automatically, constantly monitoring all online discourse and removing \*potentially\* harmful speech. And as far as I can tell, that's what this proposal does, and I oppose it in the strongest possible terms.

## Felicia Mazzarello

From: Sent: To: Jason Pickavance October 15, 2021 10:46 AM ICN / DCI (PCH)

I do not agree with anything you are doing.

Please stop this sickness.

s.19(1)

Please leave us alone.

**Jason Pickavance** 

From:	Elizabeth Marston
To:	ICN / DCI (PCH)
Subject:	Regarding the apalling new "online harms" legislation
Date:	August 14, 2021 4:30:54 PM

Hello! I'm Elizabeth Marston, a Canadian citizen who works as

I've co-created a sitcom for Canadian TV, and I've co-edited an anthology of transgender Buddhist writing.

I am deeply concerned with the proposed 'online harms' laws as documented at https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html

The new laws are poised to make Canada inhospitable to marginalized voices, while simultaneously locking in the power of the current generation of (quite dreadful) online content-arbiters.

I implore the government to read Cory Doctorow's excellent analysis here:

https://pluralistic.net/2021/08/11/the-canada-variant/#no-canada

As a marginalized Canadian, I'm presumably one of the folks these laws are intended to protect. But in reality, these laws will undoubtedly be used against the queer community, the next time the Conservative government takes power. These new proposed laws seem to have no internal checks and balances, meaning that you are placing us in harm's way. Honestly, what are you thinking?

As someone who (apparently made the mistake of) voting for the Liberal party last election, I guarantee you I will not make this mistake again.

I have no choice but to mobilize my community against this legislation and against the Liberal Party of Canada.

### Felicia Mazzarello

From: Sent: To: Subject: Christopher Deane October 22, 2021 10:48 PM ICN / DCI (PCH) BC

s.19(1)

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Christopher Deane

From:	Matt Lee Ine Access to
To:	ICN / DCI (PCH)
Subject:	Feedback on The Government's proposed approach to address harmful content online
Date:	August 14, 2021 2:59:49 PM

Hello,

Please don't do anything in this proposal. I can't sum any of the issues up better than the EFF did <u>https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filtering-blocking-and-reporting-rules-1</u>. The rules themselves won't do what you want them to do. The only effect that this will have is that all of the major social media platforms will end up geoblocking Canadian users and it will make life incredibly difficult for all of us. Personally I'd probably lose my job. Don't do this.

Matt

From:	Anish Acharya
To:	ICN / DCI (PCH)
Subject:	Harmful online content
Date:	August 14, 2021 1:39:41 PM

I strongly disagree with the new proposed law to regulate online content. It's a ham fisted approach that will irreversibly harm free speech and further marginalize the communities it seeks to serve. I strongly disagree with all aspects of this proposal.

- Concerned Canadian citizen, Anish Acharya

 From:
 All Makki

 To:
 ICN / DCI (PCH)

 Subject:
 On harmful content rules

 Date:
 August 14, 2021 1:34:34 PM

Hello,

I want to be clear that I am 100% against the proposed rules.

While hate speech is abhorrent, it must be combatted by better speech, not with censorship.

These rules effectively allow the government to decide what we can and can't read, and that is the antithesis of living in a free society.

It should not be the place of the government to decide what is hate speech, as that can vary widely by interpretation and individuals concerned.

We should all be allowed to express ourselves freely, and criticize freely without fear or repercussion.

Thank you.

From:	Perlithecat (DE AC
To:	ICN / DCI (PCH)
Subject:	"The government's proposed approach to address harmful content online"
Date:	August 14, 2021 12:52:10 PM

As a Canadian I was alarmed to learn about "The government's proposed approach to address harmful content online".

I am not going to waste breath on why this is a terrible, vague approach that will limit free expression as collateral damage to its goals.

But I with an election being announced tomorrow I will definitely NOT be voting for any party that supports this.

### Felicia Mazzarello

From: Sent: To: Subject:

October 5, 2021 9:36 PM ICN / DCI (PCH) Bill C36

s.19(1)

I remember when Canada used to be a free country! Now this is Chinada! Bought and paid for by our criminal Prime minister! Even China can't stop good VPNs!

Sincerely a Canadian leaving to retire full time in the US in under 10 years! Can't wait

 From:
 John

 To:
 ICN / DCI (PCH)

 Subject:
 This legislation is bad

 Date:
 August 14, 2021 12:45:13 PM

To whom it may concern

This bill is overly broad, gives the government to much power to punish isp's etc with to little time to moderate content. This link goes into greater detail.

https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=26385 <https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=26385>

I am not in favor of this law and will not vote for the party that passes it.

John Danton

 From:
 Cathy McIntyre

 To:
 ICN / DCI (PCH)

 Subject:
 my freedoms

 Date:
 August 14, 2021 10:46:19 AM

Stop trying to control everything we see and watch- we can make our own decisions!

Cathy McIntyre

Sent from Mail for Windows

From:	Trevor Braun
To:	ICN / DCI (PCH)
Subject:	The proposed approach to address harmful content online is bad
Date:	August 14, 2021 12:49:23 AM

The discussion guide for this proposal starts by stating that "The Government believes in supporting a safe, inclusive, and open online environment." however it fails spectacularly on all three accounts.

A combination of overly broad harmful content categories, absurdly high fines for failure to remove content, and an extremely short deadline for removal of content ensures that companies will remove vast amounts of content that is perfectly legitimate. Furthermore those most impacted by this will be the very victims of online abuse that this is supposed to be helping! Someone wanting to discuss their experience receiving hate messages or a journalist reporting on "terrorist content" may quickly find their discourse censored by a broad corporate filter just in case. In fact it explicitly requires an overly broad approach by mandating the reporting of "potentially illegal content"! Censoring victims isn't safe or inclusive, and censoring journalists certainly isn't open.

The extraordinary requirements on companies to comply (speech filters aren't cheap to create, extending data holding requirements adds further cost and increases data theft risks, and the fines are massive) further enshrines the dominant (and mostly non Canadian) large companies in this space by making it near impossible for any new entrant to compete.

Finally the proposed authority of the commissioner is an outrageous overreach of government power. Being able to enter any place for anything simply because they "believe" there to be relevant... anything, is ridiculous. Requiring someone to provide "information that the inspector considers necessary for the purpose of verifying compliance" to be turned over regardless of whether the belief they have that information has any evidence, or of the privacy or confidentiality of that information is a further absurd overreach.

These proposals throw Canadians' rights under the bus and would ruin the internet for Canadians.

Trevor Braun

From:	Brianna Price
To:	ICN / DCI (PCH)
Subject:	Concerns about "harmful content" bill
Date:	August 13, 2021 11:17:07 PM

#### Hi there,

I would like to express my concerns with the new proposed regulations around harmful content on social media sites. While I believe that many of the types of speech mentioned in the regulation are harmful and dangerous, I do not think that this sort of online regulation is going to help address them. Instead, what we have routinely seen when governments pass these sorts of laws is that those targeted are the most marginalized - especially lawful & consensual sex workers.

We need look no farther than the bills FOSTA and SESTA in the United States that this impact has had - with sex workers being run off of many platforms because those platforms use these types of regulations as an excuse to not host content that advertisers don't like. This is how these bills are used wherever they are introduced - France's was such a danger, it was ruled unconstitutional.

The wording and swiftness of this bill represent a danger to sex workers and other marginalized people, and will not actually penalize or remove white supremacist content, harassment and child pornography. These bills have been introduced in many places, and they have made little to no impact on those sorts of harms. This is not an effective or adequate approach that a government should be taking - these regulations should be worded more carefully, explicitly protect sex workers, and be made with an understanding of how social media platforms act. As it stands currently, it is set up to increase the harm these tech giants can inflict, and further marginalize sex workers.

I hope that you take people's opinions into account, and listen to what people are telling you about this bill. If you don't, you will endanger and harm those you should be protecting, and protect those who need to be stopped.

Thanks, Brianna Price

s.19(1)

### Felicia Mazzarello

From: Sent: To: Subject: Rob Moffatt September 30, 2021 8:13 AM ICN / DCI (PCH) Fwd: CAJ urges government, law enforcement to address targeted harassment of reporters

s.19(1)

------ Forwarded message ------From: Rob Moffatt Date: Thu, Sep 30, 2021 at 9:02 AM Subject: Fwd: CAJ urges government, law enforcement to address targeted harassment of reporters To: <<u>brenda.lucki@rcmp-grc.gc.ca</u>>

------ Forwarded message ------From: **Rob Moffatt** Date: Thu, Sep 30, 2021 at 9:02 AM Subject: CAJ urges government, law enforcement to address targeted harassment of reporters To: <<u>brent@caj.ca</u>>, <<u>fatima@caj.ca</u>>, <<u>zane@caj.ca</u>>, <<u>paul@caj.ca</u>>, <<u>karyn@caj.ca</u>>, <<u>anja@caj.ca</u>>, <<u>cecil@caj.ca</u>>, <<u>eilis@caj.ca</u>>, <<u>nebal@caj.ca</u>>, <<u>laurie@caj.ca</u>>, <<u>olivia@caj.ca</u>>, <<u>admin@caj.ca</u>>, < <<u>ottawa@caj.ca</u>>, People's Party of Canada PPC <<u>info@peoplespartyofcanada.ca></u>

# CAJ urges government, law enforcement to address targeted harassment of reporters

https://caj.ca/blog/CAJ\_urges\_government\_law\_enforcement\_to\_address\_targeted\_harassment\_of\_reporters

# The public urges government, law enforcement to address targeted harassment of tax paying voters

The segregation and hatred promotion belongs to the librano bribed fake news fish wrap tabloid monopolies!! Not even worthy as ass wipe during an imaginary COVID-1984 Plandemic!! You're not "journalists", you're corrupt librano puppets and parrots!! I predict a VERY bad economical future for you all if this type of antisocial behaviour from you is to continue. Remember Nuremberg!! Lest We Forget the last time you corrupt fascist dared rear your ugly faces.... Stand Firm in the Law la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act.

Document communiqué en vertu de

https://www.youtube.com/watch?v=sKzO8U5OT1A

# Vaccine Passport is all Smoke and Mirrors

https://canadafreepress.com/article-video/vaccine-passport-is-all-smoke-and-mirrors

# NEVER "trust" white coat drug pushers nor their pig pharma snake oil wares!!

Canadians haven't been getting very good value for the taxes extorted by what passes for (ahem) "governments" at any level of any party. <u>The election process is a farce and fraud.</u> These <u>organized criminals</u> and <u>social terrorists</u> pretending to be politicians stop representing and respecting those who bothered to show up for the charade the very minute the polls close. They then hop into bed with unelected lobbies, NGO and (ahem) "<u>non profit charities</u>" where our taxes are funnelled in mass for "<u>native advertising</u>" (payola fraud) pieces in "<u>social engineering</u>" (eugenics) using "denormalization" (segregation and hate) tactics to <u>"nudge" (bully)</u> "behaviour change" ("the science") under the guise of "protecting the children" (patent pending) pitting neighbour against neighbour completely destroying the very fabric of our once all inclusive society. Paid for by the very people they attack. "Honourable" and "Public Servant" are now oxymorons. We are then shut out, ignored and only viewed as cash cows to be milked and manipulated at the <u>corrupt, incompetent elite's whim</u> We are being divided and sub divided socially then pit against each other for political and financial profit. Subliminal Stalinism triumphant!

<u>"Vaccine passports/certifications" violate section 6 of the charter</u> and are unwarranted and unwanted social segregation policies that <u>turn Canada into a police state</u>. You can't hold a gun to the tax paying voters face while you pick their pockets then demand "trust" and "respect". What you will get back in kind is the exact opposite. <u>No trust and complete dis-respect accordingly</u>. They have been pitting us against each other with their unwarranted and unwanted medical/public health mafia <u>experiments in social engineering without consent</u> violating the Nuremberg code for far too long now and it needs to stop stat.

"The Just Society will be one in which the rights of minorities will be safe from the whims of intolerant majorities."

Society will do what it has to do to provide for themselves and their families. Keep a roof over their heads, feed, cloth and educate their children etc. regardless of the intolerant's policies to keep them from doing so. Society is very adaptive at ways of getting around the intolerant's not so democratic politics of fear. Fortunately, time heals all wounds but the cutting must stop now, today so the healing can begin.

<u>Canada is heading into darkness.</u> We are being divided, sub divided then pitted against each other for political/financial profit. Is now the time for the "unvacinated" and "smokers", "obese", "foreigners" and any other socially divided minority "deemed" to be a "burden", "dangerous" and "anti societal" by the "intolerant majorities" to form our own declaration of autonomy from those who only pretend to represent and respect us? All the societal rejects come together to build our own neighbourhoods, cities and countries. Grow with "refugees" (the "intolerant majorities aren't finished yet and will soon be the "minority" themselves) from the increasingly totalitarian, oppressive authorities we are currently trapped within? Render the government, the intolerant majority and etc. irrelevant, impotent and empty over time. What we have now is a farce and fraud and it's starting to get dangerous, very dangerous. We're no longer on a "slippery slope", we've gone off the cliff and there's no one at the wheel.....

Document communiqué en vertu de la Loi sur l'accès à l'information.

If the payola fraud front page bold print headline in this fake news fish wrap tabloid monopoly (largely funded with taxpayer money) is any indication of what their definition of "normalcy" is and means then they can keep it. That is a Canada I would not have anything to do with in any way, shape or form....



WEATHER HIGH 33 C | CHANCE OF THUNDERSTORMS | MAP A22

If an unvaccinated person catches it from someone who is vaccinated, boohoo, too bad I have no empathy left for the wilfully unvaccinated. Let

Canada, no longer strong nor free. Canada, life in a Banana republic....

In modern usage the term has come to be used to describe a generally unstable or "backward" dictatorial regime, especially one where elections are often fraudulent and corruption is rife. By extension, the word is occasionally applied to governments where a strong leader hands out appointments and advantages to friends and supporters, without much consideration for the law. A banana republic can also be used to describe a country where a large part of its economy and politics are controlled by foreign powers or even corporations.

The Moffatt Declaration:

1 - The federal Government of Canada is not a legitimate government.

Provincial and municipal governments within Canada are not legitimate governments.

A) Governments in Canada are not legitimate, because they support,

condone and/or engage in levying taxes upon social minorities, which

taxes are then used;

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act.

 to fund the formulation, promotion and implementation of laws and regulations that effectively deprive members of that social minority of; the safety of public and privately owned shelter, housing, employment, parental authority & custodial rights, or medical treatment.

to fund the formulation and implementation of mass-media campaigns
 which incite & promote irrational fear or hatred of the members of
 that minority among the general public.

- to fund the formulation and implementation of social marketing propaganda campaigns directed at policy-makers, both inside and outside of governments, calculated to manipulate those policy-makers into believing that it is in their own best interests and the best interests of those they represent to support the above listed scapegoating and persecution of that social minority.

 to fund and promote "research studies", lacking genuine scientific integrity and objectivity, that are calculated to generate biased data and fraudulent or unprovable conclusions supporting the social marketing propaganda mentioned above.

4

B) Governments in Canada are not legitimate, because they participate in conspiracy to deny members of scapegoated social minorities any effective means by which to air their grievances and/or seek redress for the wrongs that are inflicted upon them - including; representation by political parties, fair and equal access to mass media, complaints aired through human rights tribunals, defamation or slander lawsuits and Charter of Rights appeals.

C) Governments in Canada are not legitimate, because policy and decision-making at all levels of government is generated not through a dialog between government members and the general public but rather through a dialog between government members and "opinion leaders" unelected technocrats, 'cause' & 'issue' activists, consulting company lobbyists and small groups of economically advantaged & socially connected elitists.

D) Governments in Canada are not legitimate, because "public opinion" has been and continues to be hopelessly corrupted by a never-ending barrage of publicly funded social marketing campaigns designed to manipulate & control people's thinking and behavior.

"The will of the people" cannot be intelligibly discerned at this point in time, because what members of the public believe they know or understand about important policy issues is being manipulated and

5

controlled by the very same "opinion leaders" listed above, i.e., unelected technocrats, 'cause' & 'issue' activists and consulting company lobbyists. Governments in Canada are not legitimate, because they support, condone and fund this manipulation of everyone's thinking and behavior. Until such time as these social marketing campaigns are adequately and impartially regulated, or better still banned entirely, it will remain impossible to determine what public opinion an a given issue would be without the distorting influence of social marketing manipulation. Governments cannot legitimately claim, therefore, that their policies are "endorsed by public opinion".

2 - Our current political, judicial and social institutions are hopelessly corrupted. Because they are corrupted, it will not be possible to use them to bring about meaningful reforms.

A) It will not be possible to use our mass media to reform our mass media. It will not be possible to use our judicial institutions to reform our judicial institutions. It will not be possible to use our political institutions to reform our political institutions. Genuine and meaningful reform will only be possible when our present political, judicial and social institutions are replaced or superseded

B) The people who run our institutions mentioned above will use those institutions to block attempts to reform them. Their power (and

б

wealth) is assured by the corrupted state of these institutions and they will not hesitate to corrupt them even more if any serious effort is made to use these institutions against them. Constitutions, laws, codes of ethics - none of these can be used to stop them from doing what they are currently doing, because these people can always invoke the over-ride they have repeatedly used to corrupt our institutions in the first place - "the public good". In the corrupted system we live within today "the public good" supersedes all else, and they are the self-defined interpreters and guardians of it.

3 - Replacing our corrupted institutions "by force" is not an option.

The people who run our hopelessly corrupted institutions are masters of conflict. They like "power struggles" in any form; economic, political, ideological, legal or violent. They like conflicts because they control the means necessary to winning them. They have stacked all the conceivable 'decks' and merely await the next sitting duck to come along and attempt to beat them at their own game. The use of any kind of "force" to dislodge & replace them, whether economic, political, legal or violent, is not an option.

4 - Superseding the current system is the best option.

The best approach to dumping our present, corrupted political,

7

judicial and social institutions will be to render them irrelevant. This strategy is not just "below the radar" of our ruling elite's prepared defenses, it is right off the screen entirely. It is, at this time, something that they cannot begin to comprehend and therefore something they will be unable to take seriously until it is too lateand that recommends this strategy as highly as anything could.

Build a parallel "system", one that has been vetted of their corruptions, one that is populated by people who sincerely wish to be a part of it - rather than populated by people who have no means to escape it, as is the case with our present corrupted system. Build parallel political, judicial and social institutions created through genuinely democratic processes and models such as the BC Citizen's Assembly. Create small-scale "autonomous zones" wherein the corrupted systems have no authority and invite businesses and industries to operate within these zones on terms that are more favorable to them than what they can get in "the old Order". Develop and grow these zones with refugees from the increasingly totalitarian and oppressive institutions we are currently trapped within. Make no direct or 'forceful' challenge to the old Order, just render them irrelevant, impotent and empty over time.

5 - The first step in becoming free people once again is to declare autonomy from our corrupted system.

8

I declare my autonomy from the federal Government of Canada, the

Provincial Government of and the municipal Government of

Regional Municipality. I declare that I refute and repudiate

all illegitimate government's alleged authority over me and how I

choose to live my life.

s.19(1)

Because I am at heart a law-abiding person, I pledge to adopt the

Criminal Code of Canada statutes governing OFFENCES AGAINST PUBLIC ORDER, TERRORISM, SEXUAL OFFENCES, PUBLIC MORALS AND DISORDERLY CONDUCT, OFFENCES AGAINST THE ADMINISTRATION OF LAW AND JUSTICE, INVASION OF PRIVACY, OFFENCES AGAINST THE PERSON AND REPUTATION, OFFENCES AGAINST RIGHTS OF PROPERTY, FRAUDULENT TRANSACTIONS RELATING TO CONTRACTS AND TRADE, and WILFUL AND FORBIDDEN ACTS IN RESPECT OF CERTAIN PROPERTY as my personal code of ethics, never to be intentionally or knowingly violated by me.

I declare that I shall respect any other laws and regulations passed by any level of illegitimate government only if reason and empathy tell me that I should, on a case-by-case basis as they may arise, and only because I freely choose to do so. I am a fully adult and mature human being, I do not require legal nannies in any form to watch over me or direct my every action.

I declare that I will not be coerced into being either an active participant or passive supporter of the oppression by illegitimate governments of other autonomous persons. If that places me in violation of petty laws, bylaws or regulations enacted by illegitimate governments of any level, I will consider those laws, bylaws or

regulations to be null & void in my life.

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act.

Rob Moffatt

BANANAda

s.19(1)

 From:
 lisa bolin

 To:
 ICN / DCI (PCH)

 Subject:
 Online censorship

 Date:
 August 13, 2021 10:49:51 PM

I say a big no to this! We are a democracy and free country!

From:	Ted Reinhardt ME AC
To:	ICN / DCI (PCH)
Subject:	Re: The Government's proposed approach to address harmful content online
Date:	August 13, 2021 9:42:02 PM
Attachments:	Technical Paper - amended.pdf

Please find attached an amended document. I used an incorrect wrong word in the definition of DAO - which is Decentralized Autonomous Organization (DAO). My apologies.

Ted Reinhardt

----- Original Message -----From: "pch icn-dci pch" <pch.icn-dci.pch@canada.ca> To: "pch mg9z" · Sent: Wednesday, August 11, 2021 3:31:07 PM Subject: RE: The Government's proposed approach to address harmful content online

Hello,

This email is to confirm receipt of your email sent on August 10, 2021.

Thank you for your comments and your suggestions. We will be sure to reach out if we have any clarification or questions stemming from your input.

Thank you again

----Original Message-----From: Sent: August 11, 2021 1:22 PM To: ICN / DCI (PCH) <pch.icn-dci.pch@canada.ca> Subject: Re: The Government's proposed approach to address harmful content online

Is it possible to receive a receipt confirmation for my 10 August 21 email? Thank you.

Ted Reinhardt

---- Original Message -----From: "pch mg9z" -To: "pch icn-dci pch" <pch.icn-dci.pch@canada.ca> Sent: Tuesday, August 10, 2021 9:01:56 PM Subject: The Government's proposed approach to address harmful content online s.19(1)

Document communiqué en vertu de la Loi sur l'accès à l'information Document released pursuant to Department of Canadian Heritage the Access to Information Act 25 Eddy St Gatineau QC K1A 0S5

Via EMAIL: poh.icn-dci.poh@canada.ca

13 August 2021 [SENT]

The Government's proposed approach to address harmful content online

I am writing to offer comment on the proposed approach. Thank you for this opportunity.

Comment 1 – Web 3.0: The document fails to recognize the existence of Web 3.0 blockchain driven services and how they may be used to elude Canadian law and government oversight. Earlier this year Dfinity.org launched "The Internet Computer **(IC)**", a platform that allows for the creation of social media platforms and other applications leveraging the blockchain. The **IC** has nodes around the world at unknown locations. It makes innovative use of cryptography to ensure integrity of the platform and provide censorship resistance. The platform is intended to become a competitor to major cloud service providers (Google, AWS, Azure, etc).

In order to run an application on the platform, one only has to pay for the service to run. There is no contract, and once an application launches, it cannot easily be stopped by any entity. It is possible to write code to re-instantiate the application dynamically. Essentially trying to stop the program it would become a whack-a-mole game. There is no company to which a lawful entity could make timely representation to seek injunctive relief.

Comment 2: - Web 3.0 Self Sovereign Identity: The **IC** has enabled Self-Sovereign Identity. A person generates securely their own identification credentials and then can sign-up to different services which cannot be cross-referenced. Each service creates a separate access token that is not shared between services. While innovative, it makes it extremely difficult to attribute who is generating traffic that falls within the five categories identified in the paper.

Comment 3: Moving beyond regulating Individuals and Corporations is necessary. New applications on the Blockchain are now emerging that leverage a governance structure called a **Decentralized Autonomous Organization (DAO)**. Once a person or identifiable entity develops an application, they can transfer ownership and control to

# Document communiqué en vertu de la Loi sur l'accès à l'information

a DAO that does not exist in law, is not a corporation, and yet is capable of exerting control over its social media platform. DAO members must use the non-attributable Self-Sovereign Identity to vote.

Comment 4: Entering a premise to look at content. New Blockchain based apps are all done online. There is no one to visit and no records to see. Seems a little archaic.

Comment5 – Liquid Democracy. Dfinity has implemented an automated governance system called the Network Nervous System (NNS), whereby token holders are able to vote on issues such as adding and removing nodes, increasing rewards, and changing services. This is done algorithmically and creates Liquid Democracy.

Similarly, the Service Nervous System (SNS) is being implemented to provide a similar voting mechanism for applications whereby a proposal can be put forward for vote. I have suggested that the Dfinity NNS be capable of communicating with the SNS to advise that a complaint has been received in one of the 5 categories. Ideally, the SNS governance should kick in and present a proposal to voters of the DAO (e.g. Take down offensive comments) and respond back to the NNS saying completed or opposed.

The challenge is that the DAO may be a mix of persons from jurisdictions whose laws are different than those in Canada. The NNS, is operated by Dfinity out of Switzerland.

The Technical Document is based on a premise of centrally controlled social media. This is shifting. Distrikt and Dscvr are two examples of decentralized social media.

Comment 6: Unclear jurisdictions. It is unclear which law applies to a platform that is launched on the IC. The creator may not be identifiable, the location of the platform may be unidentifiable, and yet it may contain content that is harmful in the eyes of Canadians.

Comment 7. Web 3.0 enables the creation of decentralized social media. It has the potential to move platforms away from big tech. If the intention is to have OCS providers foot the cost for this oversight infrastructure, it will stifle decentralized social media as it does not have a revenue stream like big tech has. This will thwart the innovation and entrepreneurship that can is about to emerge with Web 3.0.

# Suggestions:

- 1. DAOs are here to stay. If a Canadian is a member of a DAO and they are aware of content that is harmful they should be required to doing something: vote to remove it and/or report it depending on a threshold.
- 2. Identifying Canadian ownership of an app is difficult. If an application is created and operated by a Canadian corporation or legal entity, it should be required to display this fact at the User Interface layer and at the API layer. It will make it easier to find to whom a platform belongs.
- 3. Any Canadian building a social media platform must be required to build in algorithmic capability to remove content contrary to Canadian law.

# Document communiqué en vertu de la Loi sur l'accès à l'information

- Any Canadian deploying smart contracts should be required to declare the legal jurisdiction for dispute resolution in the api and in the user interface.
- 5. Transnational crime and unscrupulous individuals will use the legislative vacuum to their advantage. I believe G20 nations need to establish similar mechanisms and enable collaboration.
- 6. There are a number of committees and governance bodies. It is top heavy and not efficient.
- 7. The use of DAO self-moderation and demonstration thereof should be sufficient to meet the needs of active content monitoring.
- 8. The Technical Document should include API requirements that Social Media OCS providers must implement (not tied to a technology).to facilitate timely responses.

I am available to discuss via video should you wish.

Ted Reinhardt

Ref: dfinity.org

s.19(1)

David Kukkee
ICN / DCI (PCH)
Online censorship by Government
August 13, 2021 9:07:38 PM

Regarding proposed legislation to censor online content, please be advised that I object to Government interference with freedom of speech.

If an offended party wishes to take issue on a point of law, so be it, but it is impossible for any one to safely and accurately censor online content without violating someone's rights.

This proposal will without question lead further down the path of loss of rights, and also without doubt expand into a nightmare of Government over-regulation.

There is also, importantly, the potential, actually the surety, that this additional power will be abused, and used against those who do not agree with those in power at any particular point in time.

We live in an age in which "experts" cannot be trusted. There must be freedom to question those who would deceive.

These abuses are in fact happening already, with Media and Tech Platforms, who already are doing the bidding of their preferred party in power.

Please step back and consult with some rational thinkers before proceeding down this very dark path.

Loss of freedom of expression will inevitably lead to a demoralized and depraved society, in which exceptional, talented individuals will be unable to present a voice of reason, unable to offer wise counsel, and too timid to speak the truth, for fear of reprisals.

These things are already happening in 2021.

Thankyou for this opportunity to speak, David Kukkee

## Felicia Mazzarello

From: Sent: To: Subject: Peter Welch October 5, 2021 10:24 PM ICN / DCI (PCH) Canada's approach to harmful content online

s.19(1)

Hello, I'd like to express a couple of major concerns with the government's proposed approach to regulating harmful content online (<u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html</u>).

I'm fully in favour of policing unlawful content online, but I feel the proposed approach will have major unintended consequences, and needs to be re-worked

First, this approach will make it difficult for social media companies to operate in Canada at all. Under the proposal, if they allow a post to stay up longer than 24 hours, and the government later deems that post to contain prohibited speech, the company may face a massive financial penalty. If social media companies continue to operate, they will be compelled to take down any post that **anyone** flags, to avoid this existential risk to their business.

That leads to the second concern: that trolls will simply flag every post they disagree with, knowing that social media companies will be forced to proactively remove them. Social media platforms handle billions of pieces of content every day. The content can only be monitored programmatically, not by humans, and any imperfection in the algorithm could lead to massive fines. Since the companies will err strongly on the side of caution, it may become impossible to discuss controversial topics online, like the campaign for Palestinian statehood. This concern has been raised by a wide range of progressive advocacy groups: <a href="https://www.ijvcanada.org/anti-racist-groups-concerned-canadas-proposed-online-harms-legislation-could-do-more-harm-than-good/">https://www.ijvcanada.org/anti-racist-groups-concerned-canadas-proposed-online-harms-legislation-could-do-more-harm-than-good/</a>

I respect the government's good intentions, but I urge it to target this legislation more carefully, consult more widely with advocacy groups, and make more of an effort to study the policies that have worked in other jurisdictions. Thank you for considering this feedback.

Sincerely,

Peter Welch

From: To: Subject: Date: <u>Rita Contois</u> <u>ICN / DCI (PCH)</u> This seems like a bad idea and this is why August 13, 2021 8:56:35 PM

Canada's government is poised to pass a "harmful content" regulation. It's a worst-in-class mutation of a dangerous idea that's swept the globe, in which governments demand that hamfisted tech giants remove broad categories of speech—too swiftly for meaningful analysis.

Many countries have proposed or passed rules on these lines: Australia, France, UK, Germany, India. They are all bad, but Canada's is literally the worst—as if Trudeau's Liberals sought out the most dangerous elements of each rule and combined them.

# https://twitter.com/daphnehk/status/1421120217585831938

What's in Canada's rule? EFF's Corynne McSherry and Katitza Rodriguez break it down.

https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposalcreates-filtering-blocking-and-reporting-rules-1

- A requirement to remove "lawful-but-awful" speech that is allowed under Canadian law, but effectively also now banned under Canadian law;
- 24-hour deadlines for removal, guaranteeing that platforms will not have time to conduct a thorough analysis of speech before it is censored;
- A de-facto requirement for platforms to install algorithmic filters to (mis)identify and remove prohibited expression;
- Huge penalties for failing to remove banned speech—and no penalties for erroneously taking down permitted speech—which guarantees that platforms will shoot first and probably not bother to

ask questions later;

- Mandatory reporting of potentially harmful content (and the users who post it) to law enforcement and national security agencies;
- A Chinese-style national firewall that will block websites that refuse to comply;
- Far-reaching data-retention policies that only the largest companies will be able to afford, which will create immortal, leaky repositories of kompromat on every Canadian internet user.

Even worse: the specific contours of all these rules will be determined anew with each new Parliament, who will get to appoint a new Canadian "internet czar" with the power to expand and extend the regulation's most dangerous elements.

The proposal allows Canadian cops to confiscate online services' computers if they are suspected of noncompliance—but offers them an insurance policy to avoid having their doors kicked in and their equipment seized: to adopt "advice" from the internet czar.

So not only will the internet czar—who might someday be appointed by PM Maxime Bernier or Doug Ford—get to rewrite the rules in public, they'll also be empowered to go beyond those rules in private "advice" to online services, backstopped by the threat of raids.

The Trudeau government are spinning this hard, just as they did with Bill C-10 (which included deceptive language that, on superficial examination, seemed to limit the scope of the law, but which was superceded by later clauses).

### https://pluralistic.net/2021/06/01/you-are-here/#crtc

In this case, the proposal limits regulation to "public" forums. But because the this is copied from other countries, we know there's room to declare a private chat-group public as soon as it hits a certain (unilaterally

determined) size threshold:

https://www.eff.org/deeplinks/2020/08/faq-why-brazils-plan-mandatetraceability-private-messaging-apps-will-break-users

The combination of:

- prohibiting broad, poorly defined speech categories;
- harsh penalties for underblocking; and
- requiring swift compliance without time for adequate assessment or counternotifications;

all guarantee that tech giants will block all kinds of speech.

But not all speech is equally at risk. People who are already marginalised are disproportionately likely to be censored under rules like this. That's what happened with the US's SESTA-FOSTA rule, nominally intended to prevent sexual trafficking.

In reality, the primary targets of this law became lawful, consensual sex workers, who are exposed to far more risk now that they can no longer operate forums where they trade "bad date" lists and other safety information.

https://www.eff.org/deeplinks/2018/03/how-congress-censored-internet

This discrimination is sticky, because SESTA caused the shuttering of forums where sex workers advocated for their rights. The more marginalised the speaker, the worst it is—which is why the most heavily impacted group is trans women of colour.

https://swopusa.org/blog/2015/11/12/trans-day-of-remembrance-statementfact-sheet/

As ever, Michael Geist is the absolute best authority to refer to on this. Geist has documented the "beware of the leopard"-style secrecy of the Liberals, who have taken great pains to shield this policy-making from public scrutiny.

https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/

But despite all the tactical obscurity, there IS a way that Canadians can weigh in on this, through this online consultation form. All Canadians should submit comments on this.

https://www.canada.ca/en/canadian-heritage/campaigns/harmful-onlinecontent.html

Online harms rules are a human rights disaster. They've been roundly criticised by UN Rapporteurs and civil society groups all over the world.

https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile? gld=26385

France's version—which was not as extreme as Canada's—was struck down as unconstitutional.

https://www.eff.org/press/releases/victory-french-high-court-rules-most-hatespeech-bill-would-undermine-free-expression

None of this is to say the tech giants are good for speech. They're terrible at moderation—of course they are. The problem with Facebook isn't merely that Zuck is a shitty online emperor for three billion people—it's that no one should have the job of "online emperor."

But the Canadian proposal will ensure that these tech giants are the last

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

generation of online platforms, by imposing a duty to spend hundreds of Information AcL millions of dollars on speech filters—something that only the largest American companies can afford.

This forecloses on the goal of whittling tech giants to size through interoperability, ending the possibility that co-operatives, nonprofits and startups could independently manage their own spaces that were still connected to the platforms.

https://locusmag.com/2021/07/cory-doctorow-tech-monopolies-and-theinsufficient-necessity-of-interoperability/

Canada is not alone in planning to convert the tech giants into constitutional monarchs, offering them perpetual dominance in exchange for suffering themselves to be regulated in how they rule our digital lives.

But that's a terrible vision for our online future. We don't want wise emperors running our digital world—we want to abolish emperors and give people the right to technological self-determination.

https://www.eff.org/deeplinks/2021/08/utilities-governed-empires

Source: mostlysignssomeportents

From:	Richard Kagerer
To:	ICN / DCI (PCH)
Subject:	Consultation feedback
Date:	August 13, 2021 8:49:25 PM

The Government's proposed "approach to address harmful content online" is one of the worst thought-out schemes I have ever seen a politician introduce. Michael Geist and others have done a great job describing the sheer idiocy – including how the ideas encapsulated in the proposals stomp all over norms and rights that are sacrosanct in our democracy: <u>https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/</u>

The advent of social media brought with it challenges that I agree we need to address, but you are so far off the mark with this proposal that I can't recognize it as being a remotely Canadian approach.

Be advised I will vote against any politician who supports any legislation resembling the garbage you've put together. We live in society that must remain fundamentally free, not a tyrannical state.

Kindly,

**Richard Kagerer** 

From:	G Czobel
To:	ICN / DCI (PCH)
Subject:	Government's proposed approach to address harmful content online
Date:	August 13, 2021 8:25:25 PM

To: Digital Citizen Initiative

I have the following concerns:

- Although much is made in the discussion guide of various "harms" that this regulatory
  framework is intended to address, only a fleeting mention is made of respecting freedom
  of expression, without going into any detail of how this balancing act will be
  accomplished, and what safeguards, if any, will be in place to ensure that freedom of
  expression does not become an inconvenient afterthought.
- "... a growing body of evidence shows that these benefits also come with significant harms." - how about providing references to this growing body of evidence and quantifying the actual extent in society and the nature of the "significant harms" so that it may be judged whether the need for this regulatory framework is indeed justified.. Does this proposal amount to a sledgehammer to kill a flea?
- There is already in place a system to address social harms of various sorts and degrees; this is the criminal and civil justice system. Why add a burdensome, expensive, and possibly metastasizing layer of regulatory bureaucracy on top of this for some, as yet unquantified, increase in harms of the online variety? Can't changes and funding to the existing regime be enough to address any *truly* serious harms in the online world. As for "harms" amounting to no more than slights and hurt feelings, a pandemic in its own right, just where would this end? Never is my guess.
- "The proposed legislation would create a new Digital Safety Commission of Canada to support three bodies that would operationalize, oversee, and enforce the new regime: the Digital Safety Commissioner of Canada, the Digital Recourse Council of Canada, and an Advisory Board." This is a perfect recipe for a stultifying, intrusive, nanny state type Star Chamber; hence the need to leave these matters to the existing regime with its existing safeguards against abuse and overreach.
- "New proposed legislation would also compel regulated entities to be more transparent in their operations ... entities would also be required to publish transparency reports on the Canada-specific use and impact of their automated systems to moderate, take down, and block access in Canada to harmful content." This should be done regardless of any other proposals in here; can be done without an extensive bureaucracy.

s.19(1)

Gabe Czobel

Sent with Secure Email.

### Felicia Mazzarello

From: Sent: To: Subject: Alex Lozano September 28, 2021 2:44 PM ICN / DCI (PCH) Cease and Desist from enacting tyrannical internet censorhip

s.19(1)

To the Digital Citizens Initiative,

As a concerned Candian citizen I am truly ashamed that my own country has declined and degraded to such a corrupt fall of commiting to tyranny and attempting to establish a law that prohibits freedom of speech, thought and expression, the very founding pillar of our nation.

These censorship laws must never pass. They are not only nonsense, inane, outrageous, and illogical. It's also hypocritical, autocratic, tyrannical, unjust, immoral, unconstitutional, Communistic, and the complete antithesis of what our country has stood for. Censoring regular Canadian citizens for merely having a difference of opinion, let alone criticism of a politician or political narrative or policy is not the work of a free country. It's the actions and work of a Communist dictatorship. Silencing, threatening, let alone arresting and jailing people for a difference of opinion and thought is a grotesque abuse and assault of people's natural humanity to think for themselves.

I personally will NEVER stand for it. I, just like millions of other Canadians, will never stand for tyrannical repression. The Canadian Charter of Rights & Freedoms exists for a reason and will be upheld to the fullest extent.

Accordingly, I call upon the incumbent government and demand that they retract, cease and desist from enacting such arbitrary, archaic, and egregious laws against free speech, for which our nation stands for.

Signed,

Alex L., concerned and enraged Canadian citizen.

From:	Benoit Jauvin-Girard the Access to Information
To:	ICN / DCI (PCH)
Subject:	Commentaire négatif sur l'approche proposée du gouvernement pour s'attaquer au contenu préjudiciable en ligne
Date:	August 13, 2021 7:54:19 PM

Je suis citoyen canadien et informaticien et je suis opposé à la démarche décrite au lien Web

https://www.canada.ca/fr/patrimoine-canadien/campagnes/contenu-prejudiciable-en-ligne.html <https://www.canada.ca/fr/patrimoine-canadien/campagnes/contenu-prejudiciable-en-ligne.html>, pour "s'attaquer au contenu préjudiciable en ligne".

Selon l'analyse de l'Electronic Frontier Foundation, dont l'expertise sur l'interaction des droits humains et de l'internet est indisputable, ce projet est une catastrophe, telle une collection des pires idées existantes pour réglementer les communications électroniques!

Au lieu de reprendre leurs arguments, je vous invite à les lires vous mêmes:

https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filtering-blocking-and-reportingrules-1

<a href="https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filtering-blocking-and-reporting-rules-1">https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filtering-blocking-and-reporting-rules-1</a>>

Les possibilités d'abus sont claire, l'article est pratiquement un manuel pour un futur gouvernement autoritaire.

Donc sachez que je m'oppose pleinement à cette approche, et ne pardonnerai jamais le gouvernement courant si elle est implémentée.

Benoit Jauvin-Girard

août 2021

s.19(1)

From:	Andrea Mrozek
To:	ICN / DCI (PCH)
Subject:	Government"s proposed approach to address harmful content online
Date:	August 13, 2021 7:51:20 PM

To the Digital Citizen Initiative:

I am responding to your request for written submissions on the proposed approach to online harms.

I would like to outline some concerns I have about the proposed approach, which will be ineffective at combating online harm and instead will capture non-criminal content and limit free expression.

I support efforts to remove criminal content from the internet. But the proposed approach will not achieve this goal, and it is unbalanced because it does not reflect concern for the fundamental rights of Canadians.

The proposed 24 hour takedown requirement will lead to platforms proactively removing noncriminal content in order to avoid massive financial penalties. This chilling effect is dangerous to free expression in Canada.

The mandatory police reporting proposal will result in the use of artificial intelligence to proactively monitor Canadian's speech, and AI generated records are likely to include non-criminal speech. I oppose this proposal, which could result in computer generated records of non-criminal speech being proactively sent to police.

The proposal includes three new regulatory bodies, which is an enormous new bureaucratic undertaking. I oppose empowering these bodies to conduct broad inspections, including warrantless inspections of non-regulated businesses. This proposal is too broad. Please take it back to the drawing board.

Andrea Mrozek Senior Fellow 613.241.4500 x.503 amrozek@cardus.ca 45 Rideau St · Ottawa ON, K1N 5W8

#### Felicia Mazzarello

From: Sent: To: Subject: Tyler Burkart - s.19(1) September 26, 2021 2:30 PM ICN / DCI (PCH) Censoring social media is a infringement on Canadians right to free speech.

Hi my name is Tyler Burkart. It is my opinion that any sort of censorship on any social media sites is a complete an over step of your rights as a government. This does not protect people. When you take away peoples rights to have their own opinion and to share it through different avenues such as social media Platforms. I feel as though you were taking the democracy out of democracy. Everyone has a right to their opinion no matter how hateful no matter how wrong, it is theirs and it is there's alone. Censorship of social media platforms is the beginning of the end for free speech as we know it. People need to be allowed to make their own choices And come to their own conclusions regardless of where they choose to get their information and regardless of whether it is truthful or not. Every person has a right to their own opinion and should have the right to express it to the world anyway they so choose so long as no physical harm comes of it. We are the stewards of our own mental health and we choose to allow or disallow information we receive which is part of the greatness of this country. The ability to seek out different and varying opinions is the essence of freedom and is what makes our country so great. The ability to share your opinion without the fear of persecution by law or by your fellow man. It is up to adults to use their own Filter for the information that we receive on a daily basis whether that be social media or your local news station or the news paper. It is there for my personal opinion that taking away the right to choose or the right to filter information is nothing but a hinderance on the freedoms and the democracy of our country. If you are a true Canadian if you are true leaders you will scrap this idea and throw it in the garbage because it is so far from Canadian, it is so far from freedom that even hearing about you considering this disgusts me in a way I cannot even express in words. Do the right thing stand up for freedom of speech and freedom of expression don't let your country down. Also it would seem to me that censorship of any information Would be a crime In my eyes. It is also opening up the door for people of tyrannical mindsets to be able to do horrible atrocities in this country while having people believe otherwise or whatever it is that you so choose to have covered by the media or censored on social media. To allow this censorship idea to become a reality you are saying you do not support freedom you do not support free-speech you do not support creativity and you do not support your people and they're right to share whatever they so choose with the world around them.

Be a Advocate for the right to choose. Choose freedom. Sincerely Tyler Burkart.

Sent from my iPhone

From:	Steven Ensslen
To:	ICN / DCI (PCH)
Subject:	Harmful Online Content
Date:	August 13, 2021 7:38:01 PM

I oppose the <u>Harmful Online Content proposals</u>. I believe these proposals to be unwarranted and unreasonable limitations of our Human Rights. I agree with the <u>Canada Research Chair in Internet and</u> <u>E-commerce Law</u> and <u>the EFF</u> that these proposals are incompatible with the <u>Charter of Rights and</u> *Freedoms* and the <u>International Covenant on Civil and Political Rights</u>.

I request that the proposals be abandoned as fundamentally anti-democratic, and that completely new proposals which prioritise free speech and minimise the requirements for new media be drafted for public consultation.

Steven Ensslen

 From:
 Geoffrey Greatrex

 To:
 Mona.Fortier@parl.gc.ca; ICN / DCI (PCH)

 Subject:
 Legislation proposed Bill C-36

 Date:
 August 13, 2021 6:28:21 PM

I am writing to you to express my serious concerns about the sweeping powers accorded the Digital Safety Commissioner in this bill, as well as by the wide scope of the measures and the potential impact they might have on free speech. While it is true that there is a great deal of dubious material on the internet, some of which clearly ought to be subject of legislation, I fear that the net is being cast very widely indeed, as Michael Geist has pointed out:

https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/

I look forward to hearing from you.

Yours,

**Geoffrey Greatrex** 

s.19(1)

Prof. Geoffrey Greatrex Directeur/Chair Dépt. d'études anciennes et de sciences des religions Dept. of Classics & Religious Studies Université d'Ottawa/University of Ottawa 55 av. Laurier est/Laurier Ave. East Ottawa, Ontario CANADA K1N 6N5 Tél. 613-562-5808 (en temps normal/normally) Fax. 613-562-5991 (pareillement/similarly)

 From:
 Will Cheney

 To:
 ICN / DCI (PCH)

 Subject:
 The proposed implementation is terrible

 Date:
 August 13, 2021 5:27:43 PM

Hello,

The proposed legislation is antithetical to everything Canada claims to stand for. It's a close cousin of totalitarian censorship than anything that could reduce harm to individuals online. It stifles free speech and a Canadian's right to free expression. It promotes a shoot first ask questions later approach to content removal, removes competition and creates an online database which is a disastourous future data leak in waiting. Finally provides the perfect tool for a future demagogue to spread propaganda throughout Canada.

No other developed democracy has passed legislation anything close to this, in fact more water downed versions are frequently found unconstitutional.

Will

From:	Denise Ferris
To:	ICN / DCI (PCH)
Subject:	Government proposal to censor and regulate speech online in Canada
Date:	August 13, 2021 4:10:16 PM

Good afternoon,

With regards to the proposal to regulate and censor speech online in Canada-

This will not be tolerated.

You will not take away our Rights and Freedoms. You will not spit on the graves of the men and women who have spilled blood and died for *our*, yes mine AND your freedoms. We will not fall towards nor be pulled into your nazi zionist communistic totalitarian goals. People in the know are very much aware of what the compromised governments of the world, sadly, including Canada are colluding to.

Let us be very clear, those in the Canadian government work for the people, let me reiterate that again, those in government positions represent, and therefore work for the ideals, betterment and positive loving care of every Canadian person. Those who are in government positions who do not follow the ideals just listed of how every government official ought to try to attain to be, will soon find themselves in a predicament that will not bode well for them. Service to others, not service to self.

I strongly urge those who have influence and are in positions to affect real change, please, be very very mindful of your part in history that is currently being played out. You will not be forgotten when the time comes and you are asked, and what did you do to help/save Canada from the great communism attack? (digital world war 3 – because that is what we are in). There is nowhere for the people who aid in the takeover of Canada to hide.

We will not have our rights and freedoms taken away from anyone.

Thank-you for your time.

Regards,

Denise Ferris

## Felicia Mazzarello

From: Sent: To: Subject: Marianne Walters October 1, 2021 11:53 PM ICN / DCI (PCH) Censorship

s.19(1)

Regarding this censorship legislation proposed

and the right to freedom of speech is in our constitution. Who decides what is ok and not ok ? Isn't that always the issue with censorship ? Exactly what are those who want to suppress information afraid of ? That their narrative is questioned , assessed and debated? Isn't that what living in a democracy is all about ?

When one group controls the media , as they do now (except for a few platforms ) , this nation is no longer a democracy...in Germany, Hitler controlled the media and his propaganda was accepted and hence he gained control of virtually all the German People. Isn't this exactly what this censorship legislation is intended to do?

We already have far too much government propaganda and far too little actual a scientific and medical discourse on the subject this is intended to suppress even more.

I feel sold out by my government , whom I have supported my entire life.

A Concerned citizen of Canada

Sent from my iPad

Neil McKellar
ICN / DCI (PCH)
heather.mcpherson@parl.gc.ca
Comments on proposed harmful online content regulations
August 13, 2021 2:56:24 PM

Hello,

I have been reviewing the material posted by the Canadian Heritage Ministry regarding narmful content online. After reviewing the discussion guide and the technical paper, I felt compelled to send you my comments. As proposed, I strongly believe the framework leads to poor outcomes. It creates incentives for a more monopolistic Internet. It will lead to greater censorship of speech.

The guidance disproportionately impacts smaller sites or startups trying to launch competing services. Network effects already make it difficult for users to switch platforms. Regulatory requirements, including rapid assessment and response, are an incentive for small sites to host with a larger platform instead, even if the operator disagrees with the terms of service or the privacy guarantees of the larger platform.

Operators have an incentive to respond rapidly to reports based on the 24-hour time limit. This creates a bias toward removing content with little assessment. Social media platforms often take down content meant to provide commentary, support journalism, or host archival evidence.

https://www.reuters.com/technology/exclusive-twitter-sees-jump-govt-demands-removecontent-journalists-news-outlets-2021-07-14/

https://www.publicknowledge.org/blog/the-online-censorship-machine-is-revving-up-hereare-a-few-lessons-learned/

https://www.nytimes.com/2019/10/23/opinion/syria-youtube-content-moderation.html https://www.hrw.org/sites/default/files/media\_2020/09/crisis\_conflict0920\_web\_0.pdf

The framework can be abused to censor speech. There is almost zero cost or obligation on reporting content. Indeed, the framework does not require collecting as much information about who flags content as it does about who posts content. A person or organization could use the regulation to keep unwanted content offline through repeated flagging and imposing high costs to appeal takedowns. High report volumes also impose costs on operators, who have no recourse but to respond to every report, however frivolous.

Finally, I believe automation will amplify bias online. Rapid assessment and removal will lead to automated scanning. The major platforms are the only organizations able to make significant investments in the natural language processing technology required. Still, there are numerous examples of false positives and overly aggressive content identification. It is not the average person who is generally impacted. Instead, it's researchers, freelance writers, activists, independent artists, and marginalized communities — basically, people with less political and economic ability to defend themselves.

https://www.forbes.com/sites/johnkoetsier/2020/03/17/facebook-deleting-coronavirus-postsleading-to-charges-of-censorship/?sh=4dabe32a5962 https://techcrunch.com/2020/03/16/youtube-warns-of-increased-video-removals-during-covid-

<u>19-crisis/</u> https://twitter.com/twittersupport/status/1308853643144241152?lang=en

I'm concerned that the framework will centralize content controls with the major platforms and lead to increased censorship. Despite its stated intentions, it will bias discourse away from marginalized communities, stifle research, and impede activism. When developing the legislation, I ask the ministry to consider its power to create incentives and look at the history of automated scanning and algorithmic bias.

Neil McKellar.

s.19(1)

 From:
 reema tarzi

 To:
 ICN / DCI (PCH)

 Subject:
 preserve an open and democratic Internet

 Date:
 August 13, 2021 2:46:24 PM

**Digital Citizen Initiative** 

Your proposal to address what you call 'harmful' online content is an outrageous and dangerous attack on free speech, privacy and the right of Canadians to access information.

I do not want politically appointed bodies policing speech. That is absolutely undemocratic.

Please consign this terrible proposal to the scrap heap where it belongs.

Regards Reema Tarzi s.19(1)

### Felicia Mazzarello

From: Sent: To: Subject: Elisabeth Rondinelli <elisabeth.rondinelli@acadiau.ca> October 1, 2021 9:49 AM ICN / DCI (PCH) Consultation on harmful online content

Hi there,

My name is Elisabeth and I'm a professor of sociology at Acadia University who studies gender-based online violence. I'm writing to ask about the status of the consultation process for addressing harmful online content. Will the public consultation documents be made public? Also, at what stage is the consultation process at? I'm curious because I'd like to track how this exciting legislation unfolds, and how it is received. Thanks,

Elisabeth

44

Elisabeth Rondinelli Assistant Professor Department of Sociology Acadia University

 From:
 Rock I

 To:
 ICN / DCI (PCH)

 Subject:
 Censorship in a democracy?

 Date:
 August 13, 2021 2:32:03 PM

Your government's wish to convertly sell us on the notion of gvt overreach of the world wide web .... is nothing short of a totalitarian dictatorship....

The Globalist marxist takeover of our democratic institutions is utterly disgusting, we can clearly see with our eye and hear with our ears, your repeated propaganda, lies, purposely deceiving and misinforming the peasants...

You Globalist shills will be held responsible for your lies and deceptions

Roch Laplante

Sent from my iPhone

 From:
 SirLance2020

 To:
 ICN / DCI (PCH)

 Subject:
 Online Speech

 Date:
 August 13, 2021 2:27:58 PM

Considering all the crimes the PM has committed and his general view of things, it's pretty apparent he's and authoritarian that can't stand criticism - like all dictators. He also needs to get rid of free speech to cut off any criticism of The Great Reset. He'd never get it through otherwise.

Biil C-10 on particular is a gross violation of our Charter Rights. Secret Trials? That's a criminal offence; Breach of Trust by a Public Officer. Let's hope the courts allow my charges to proceed, otherwise, it could lead to civil war, as we're at the Point of No Return on the Tytler Cycle already.

Lance Humphries SirLance.ca

s.19(1)

Sent with ProtonMail Secure Email.

 From:
 Marcello Pavan

 To:
 ICN / DCI (PCH)

 Subject:
 The Government's proposed approach to address harmful content online

 Date:
 August 13, 2021 12:54:53 PM

Simple: stop this nonsense proposal ASAP, if not sooner.

Start over. Please do not worry about losing face - just say you listened and all will be forgiven

-Marcello Pavan

Sent from my iPad

s.19(1)

Sean Cocks
ICN / DCI (PCH)
harmful content online
August 13, 2021 12:37:11 PM

When are we going to learn? Algorithmic censorship does NOT work. It will NEVER work. It will always overblock legitimate content, silencing minority voices, and handing all control over online discussions to companies huge enough to deal with it. You want the internet to only be facebook and google? And make no mistake, these huge companies have no interest in protecting free speech; they will end up blocking all kinds of marginalized people, legitimate satire or fair use, making the net extremely homogenous and useless, while still somehow letting child porn and fascists get their stuff out there.

I'll just say it again - algorithmic censorship of online content will never work. Never. You'll just end up handing over all online discussion to Facebook and Google, and they will squash everything. We'll all be trapped in their "walled garden", reading only what they want us to read and saying only what they permit us to say. Stop this now.

-> sean

From:	Ariana Feltrin	
To:	ICN / DCI (PCH)	
Subject:	The Government's proposed approach to address harmful content online	
Date:	August 13, 2021 12:03:22 PM	

#### Digital Citizen Initiative,

I am writing today to express my immense displeasure towards the Government's proposed approach to address harmful content online. Trying to protect vulnerable people online is noble in theory, but with the proposed methods it will do the opposite. Similar efforts have become laws in other countries and have proven themselves to be incredibly dangerous to marginalized people. These proposed actions violate human rights and remove platforms and resources from the vulnerable. Only social media giants will be able to afford the proposed fines so any company that cannot will cease to exist having negative impacts on the Canadian economy. The vague language of the proposed approach means what is deemed as harmful isn't clearly defined and may change. Companies are not given enough time to review content for context and will therefore take a broad-sweep approach to removing content. They are also required to report users to law enforcement, which is incredibly dangerous for marginalized people, and ludicrous as they may not have broken any laws. This is proposed mass censorship and it is very disturbing that people in power actually thought this was a good idea.

Ariana Feltrin

 From:
 Frank Adamek

 To:
 ICN / DCI (PCH)

 Subject:
 Censorship

 Date:
 August 13, 2021 11:29:46 AM

The main purpose of the censorship is to prevent public criticism of the liberal party. Censorship is common to all dictatorships, and only to dictatorships. Is Canada headed that way?

Frank Adamek

s.19(1)

 From:
 ICN / DCI (PCH)

 Subject:
 regulating online speech

 Date:
 August 13, 2021 11:00:41 AM

I cannot see any good in regulating online "speech", except that which contravenes existing law. Free and unrestricted speech is a cornerstone of democracy and is under threat from many quarters.

s.19(1)

Please. Back off.

Helen Yeomans

 From:
 Alan Adelstein

 To:
 ICN / DCI (PCH)

 Cc:
 laurel.collins@parl.gc.ca

 Subject:
 THIS IS A TRILLION TIMES A TERRIBLE IDEA

 Date:
 August 13, 2021 10:56:45 AM

# O (No!) Canada: Fast-Moving Proposal Creates Filtering, Blocking and Reporting Rules—and Speech Police to Enforce Them

https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filteringblocking-and-reporting-rules-1

 From:
 alezz cole

 To:
 ICN / DCI (PCH)

 Subject:
 We will not accept your online censorship

 Date:
 August 13, 2021 10:56:28 AM

You government officials are a disgrace, we live in a free country. You don't have the right to censor the internet. We dont live in nazi germany, canada is a free country. We have the right to free speech and speak our concerns with what is going on in the world.

From:	Tess Kitching	
To:	ICN / DCI (PCH)	
Subject:	The Government's proposed approach to address harmful content onli	
Date:	August 13, 2021 10:42:03 AM	

Hi there,

s.19(1)

I'm not particularly articulate, but I live in and would like to voice my opinions on the proposed legislation regarding harmful content online.

This article sums up my feelings very well: <u>https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filtering-blocking-and-reporting-rules-1</u>

Particularly this section: "Indeed, it seems like the people who drafted this policy themselves looked to other countries for inspiration—but ignored the criticism those other policies have received from human rights defenders, the UN, and a wide range of civil society groups. For example, the content monitoring obligations echo proposals in India and the UK that have been widely criticized by civil society, not to mention three UN Rapporteurs. The Canadian proposal seeks to import the worst aspects of Germany's Network Enforcement Act, ("NetzDG"), which deputizes private companies to police the internet, following a rushed timeline that precludes any hope of a balanced legal analysis, leading to takedowns of innocuous posts and satirical content. The law has been heavily criticized in Germany and abroad, and experts say it conflicts with the EU's central internet regulation, the E-Commerce Directive. Canada's proposal also bears a striking similarity to France's "hate speech" law, which was struck down as unconstitutional."

While I certainly understand that the goal is noble, the means by which you want to go about it are way too extreme. This amount of censorship could easily lead to far more harm than good, and end up harming people who are looking for support or trying to comment about their own abuse, and lead to restrictions like China has. Plus, 24 hour turnaround is way too little time for things to actually be properly assessed; sites like Facebook and Twitter take weeks to investigate claims already, forcing them to try and review things in under 24 hours will just lead to them deleting them without review, which will just lead to people spam reporting accounts they don't like just to get them shut down. This already happens, to be clear, but it would force it even further.

Please reconsider and look at plans that are less strict. To be quite frank, the proposed bill comes across as rather draconic and authoritarian, more like something people would see in China or North Korea than a free, Democratic country like Canada.

Please read the article I linked in full for further reasoning as to why the current proposal goes too far and, in fact, may cause legal issues.

Again, I do absolutely understand the desire to remove harmful content from the internet, and as a woman, trust me, I've seen and experienced plenty of harassment myself that should never have been allowed. However, the proposed legislation goes too far, and will actually empower abusers rather than their victims.

Please reconsider. - Tess Kitching Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act.

#### Felicia Mazzarello

From: Sent: To: Subject: Micah -October 5, 2021 6:20 PM ICN / DCI (PCH) Digital Citizen Initiative - Government's proposed approach to address harmful content online

I disagree with these laws that attempt to limit free speech, interaction. I agree catching child pornographers and terrorists sounds great, but in the end these laws are always used to catch those who are not either or something else. Soon anyone dissenting government viewpoints will be considered domestic terrorists as has happened in the US media.

These laws are not acceptable. Micah s.19(1)

 From:
 Gabriella Liberatore

 To:
 ICN / DCI (PCH)

 Subject:
 Proposal to censor and regulate speech online

 Date:
 August 13, 2021 10:38:26 AM

With reference to the above noted subject, and the proposal to install a law towards this. If our government were to be trusted (obviously they can't), they would only initiate appropriate action towards illegal content. Unfortunately since our government, as we have learned through this whole ordeal, is that they cannot be trusted and have their own personal agendas. Canada's government should not be given cart blanch on Canadians freedoms of speech. To do so would change our democratic society and slowly turn it into a dictatorship, which I and so many others know that this is what Trudeau wants.

Our government has accomplished so much civil unrest, that if this continues people will be pushed too far and will retaliate. It's starting to feel like Nazi's Germany during WWII. Canadians are very compliant and that is what Trudeau is banking on, but everyone can only be pushed so far before they break.

If this law goes through the repercussions will be felt for years. Canada has always looked attractive on the world front, but not anymore, the world is now seeing what we are living, and no one in their right mind would want to visit or live here.

Sincerely Gabriella Liberatore

From:	Christopher Lord (NE ADDESS 10
To:	ICN / DCI (PCH)
Subject:	Illiberal policies: The Government's proposed approach to address harmful content online
Date:	August 13, 2021 9:42:09 AM

You are forcing me to be a single issue voter, your proposal to restrict speech in arbitrary ways with poorly defined terms like "hateful" is so illiberal that I am going to make it my single issue in the next election and I will be recommending that all of my liberal (small 1) friends do the same. We will tactically vote you out and install whoever promises to repeal this. There is literally no more important issue to me, for this is the bedrock of our civilization.

The question comes down to semantic creep. It used to be that violence was something physical. Now it's creeped up to something else. Same with hate. I hate my choices for political parties. Does that classify as hate speech? Tune in next week!

This fascist authoritarian behavior will have consequences for the Liberals. It will unite the conservatives and liberals at the very least, and might bring a wave of anti elitism that will change Canadian politics for a generation. Your call: embrace authoritarianism or embrace liberalism.

Christopher

### Felicia Mazzarello

From: Sent: To: Cc: Subject: Rob Nourse October 5, 2021 12:58 PM ICN / DCI (PCH) PM@canada.ca Digital Citizens Initiative feedback

s.19(1)

Guys,

This legislation is absolutely riddled with problems which even I can see and I have zero experience with legislation. That alone should be ringing alarm bells all over Ottawa.

Firstly the way this is written is going to result in one of two things... either the social media platforms of the day will over-censor in an effort to avoid being the targets of litigation which will result

In thousands of innocent Canadians facing charges or they'll leave Canada entirely based on ridiculous penalties which make operating in this country a liability shareholders won't tolerate.

Seriously... did anyone with experience actually read through this?

This needs to be scrapped and done over. Draft 1 as outlined is a clear "swing and a miss"

**Rob Nourse** 

 From:
 Yuri Runoff

 To:
 ICN / DCI (PCH)

 Subject:
 Re: Censor and regulate speech online in Canada

 Date:
 August 13, 2021 8:22:25 AM

Hi,

This censorship (bill C-10) is a clear path to socialism and to the new Soviet Union. This must be stopped.

We already lost our free media (which now are controlled by 600 mln fund with an 'independent' board), and online censorship will kill another our fundamental freedom.

Kind regards

Yuri Runoff



s.19(1)

Canada

 From:
 ICN / DCI (PCH)

 Subject:
 Comments: harmful content regulation

 Date:
 August 13, 2021 7:58:48 AM

I am writing because I am very concerned about the harmful content rules that the Canadian government is working on. I agree that harmful and hateful content is bad for society, and we should be doing something collectively to help prevent young and vulnerable people from being radicalized. I disagree with the approach the government is taking to solve it in a way that will suppress citizens ability to "speak". Setting up China style censorship will be very bad for our country and it does not represent the values of Canadians. I think the correct path is to increase investment into the education and success of our youth.

Sincerely,

Russel Ward

s.19(1)

From:	Bryan Heystee
To:	ICN / DCI (PCH)
Subject:	Hateful content online
Date:	August 13, 2021 7:40:39 AM

The Canadian government's proposal to manage, limit, and/or eliminate hateful online content is ill-conceived, will be ineffective, and will have adverse consequences that are contrary to the interests of everyday Canadians. Not only will it not effectively eliminate the hateful content, it will unduly limit and suppress legitimate content and will marginalize already disadvantaged people. Furthermore, it will cement the digital oligopoly that already does great harm to our digital lives by ensuring American mega-corporatations - Facebook, Google, etc -will be the only ones to meet the poorly conceived requirements the government is proposing.

Bryan Heystee

Sent with Secure Email.

s.19(1)

 From:
 Wayne Currle

 To:
 ICN / DCI (PCH)

 Subject:
 Internet censorship

 Date:
 August 13, 2021 12:22:14 AM

Your intent to censor information on the Internet is deeply disturbing. It flies in the face of freedom of speech and is detrimental to the exchange of data and ideas. Are the leaders of this country so insecure that they cannot withstand scrutiny or criticism? Please rescind this proposed censorship.

Wayne Currie

 From:
 Tracy

 To:
 ICN / DCI (PCH)

 Subject:
 No to Govt

 Date:
 August 12, 2021 9:01:47 PM

Govt has no business "regulating" people's lives. Govt serves the people, not the other way round. The people say no to govt & will vote in a new one.

#### Felicia Mazzarello

From: Sent: To: Subject: Terry Chiasson < s.19(1) October 29, 2021 3:46 PM s.19(1) ICN / DCI (PCH) Government's proposed approach to address harmful content online

To the Digital Citizen Initiative.

I am responding to your request for written submissions on the proposed approach to online harms. I would like to outline some concerns I have about the proposed approach, which will be ineffective at combating online harm and instead will capture non-criminal content and limit free expression.

I support efforts to remove criminal content from the internet. But the proposed approach will not achieve this goal, and it is unbalanced because it does not reflect concern for the fundamental rights of Canadians.

The proposed 24 hour takedown requirement will lead to platforms proactively removing non-criminal content in order to avoid massive financial penalties. This chilling effect is dangerous to free expression in Canada.

The mandatory police reporting proposal will result in the use of artificial intelligence to proactively monitor Canadian's speech, and AI generated records are likely to include non-criminal speech. I oppose this proposal, which could result in computer generated records of non-criminal speech being proactively sent to police.

The proposal includes three new regulatory bodies, which is an enormous new bureaucratic undertaking. I oppose empowering these bodies to conduct broad inspections, including warrantless inspections of non-regulated businesses. This proposal is too broad, and may violate the right to be free from unreasonable search.

I am concerned by the proposal to allow the Digital Recourse Council to conduct secret hearings. This goes against the open court principle and basic notions of democracy. I am also opposed to the new proposed power that this regulator would have to block websites.

Instead of addressing criminal content, this proposal will drive the content underground to more obscure platforms. I am concerned that the impact of this proposal will be to silence non-criminal expression by everyday Canadians using these platforms.

Please take this plan back to the drawing board.

Yours truly,

**Terry Chiasson** 

From:	Black Sheep Clan
To:	ICN / DCI (PCH)
Subject:	Censorship
Date:	August 12, 2021 8:59:10 PM

No to censorship

Govt needs to stop being Big Daddy to us and deciding what or what not is good for us We can decide for ourselves and our families. Stop Censorship! Stop Censorship! Stop Censorship! 100 %.. stop! D. Leonne

s.19(1)

From: To: Subject: Date: Nell Palesh ICN / DCI (PCH) Comments on the Government's proposed approach to address harmful content online August 12, 2021 8:53:30 PM

Hello

I reviewed the discussion guide (<u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html</u>) and technical paper (<u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html</u>) on the harmful online content initiative and am sending this email to provide my comments, as an individual Canadian, part of the public consultation process:

- I am very concerned about how the approach proposed (in full or part) infringes on all fundamental freedoms in the Canadian Charter of Rights and Freedoms. The monitoring proposed through the approach amounts to wire-tap for phone lines and entering private spaces without a warrant. It is never appropriate for the government to attempt to regulate thought and discussion, only when actions actively case harm to someone;
- The distinction between entities that come under regulation or are exempted is not sufficiently detailed. For example, Facebook operates a full circle social media enterprise which incorporate private conversation (Messenger and WhatsApp) as well as permission-based conversation (friend networks and groups), and fully open communication (public posts on a wall.) Similar ambiguity exists with other large platforms that support robust sharing permissions. If regulation is sought it should only apply to fully public spaces and in a similar manner as it would in a real-life sphere where people would put up posters or assemble in protests and demonstrations. Even in these public open spaces a wide variety of content is tolerated so long as it isn't hate crime;
- Private organizations err on the side of caution since they're risk adverse to litigation. This would result in over moderation and stifling of harmful content or content classified incorrectly;
- Part of allowing "harmful content" is a feedback loop and education piece that happens in society. If harmful content is supressed or actively punished not only will it drive these people underground and to perform worse acts, but it also removes the rehabilitative effect open community and discussion can have in how these actors inform their views; and
- Additional regulatory burden might drive away social media innovation and options in Canada which on the whole leave Canadians behind other nations where free and open discussions are not subject to regulatory oversight.

A free and democratic society does not oppress views that are repugnant or harmful, but rather engages them at their level with the intention of betterment for the individual and community. Canada has sufficient legislation to deal effectively with hate crimes and a well-

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

developed human rights landscape. Additional regulation of harmful content is not required on Act and is incongruent with fundamental freedoms in our Charter. The modules proposed in this consultation are not necessary and should be abandoned.

Best Regards Neil Palesh

From:	Marilyn Mackay
To:	ICN / DCI (PCH)
Subject:	No to Censorship
Date:	August 12, 2021 8:23:23 PM

To whom it may concern:

When government leaders and influencers censor those who question, disagree, challenge or debate political policies and narratives/dogma which are unsupported by data, this is dangerous for democracy and the health of our. nation. Policies driven by money and coercion, do not serve our population's rights and freedoms in Canada. Free speech is important for a productive, safe, balanced, and vibrant society.

Sincerely, M. Mackay

## Felicia Mazzarello

From:	Rhiannon Beaudry	
Sent:	October 27, 2021 4:08 PM	s.19(1)
To:	ICN / DCI (PCH)	
Subject:	Government's proposed approach to ac	dress harmful content online

To the Digital Citizen Initiative.

I am responding to your request for written submissions on the proposed approach to online harms. I would like to outline some concerns I have about the proposed approach, which will be ineffective at combating online harm and instead will capture non-criminal content and limit free expression.

I support efforts to remove criminal content from the internet. But the proposed approach will not achieve this goal, and it is unbalanced because it does not reflect concern for the fundamental rights of Canadians.

The proposed 24 hour takedown requirement will lead to platforms proactively removing non-criminal content in order to avoid massive financial penalties. This chilling effect is dangerous to free expression in Canada.

The mandatory police reporting proposal will result in the use of artificial intelligence to proactively monitor Canadian's speech, and AI generated records are likely to include non-criminal speech. I oppose this proposal, which could result in computer generated records of non-criminal speech being proactively sent to police.

The proposal includes three new regulatory bodies, which is an enormous new bureaucratic undertaking. I oppose empowering these bodies to conduct broad inspections, including warrantless inspections of non-regulated businesses. This proposal is too broad, and may violate the right to be free from unreasonable search.

I am concerned by the proposal to allow the Digital Recourse Council to conduct secret hearings. This goes against the open court principle and basic notions of democracy. I am also opposed to the new proposed power that this regulator would have to block websites.

Instead of addressing criminal content, this proposal will drive the content underground to more obscure platforms. I am concerned that the impact of this proposal will be to silence non-criminal expression by everyday Canadians using these platforms.

Please take this plan back to the drawing board.

Yours truly,

Rhiannon Beaudry

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

This email, including attachments, is solely for the use of the intended recipient(s) and may contain confidential and/or privileged information. Any use, distribution, printing or copying of this email must comply with Rainbow District School Board's procedure on the <u>AP - Acceptable Use of Information</u> and <u>Communication Technologies</u>. If you have received this email in error, please delete it immediately from your system and notify the originator.

Dwight Williams
ICN / DCI (PCH)
Marie-France Lalonde
The Online Harms Proposal
August 12, 2021 8:19:54 PM

Hello.

Since we were all asked for our opinions on this idea?

Frankly, I think that while there are real issues of public safety we need to keep working on, this proposal worries me. When I look at the authoritarian turns too many of the other nations of this planet have been taking over this past ten to twenty years, I am reminded that national governments always change hands eventually. Always. And this proposal - if implemented as is - can be made to backfire. There are people already positioned to pervert the tools they'll be handed.

Please take this back to the drafting table. It may well be that Canada doesn't need its own version of a "Great Firewall".

**Dwight Williams** s.19(1)

 From:
 Brad

 To:
 ICN / DCI (PCH)

 Subject:
 Bad bad bad

 Date:
 August 12, 2021 7:58:14 PM

"Canada's government is poised to pass a "harmful content" regulation. It's a worst-in-class mutation of a dangerous idea that's swept the globe, in which governments demand that hamfisted tech giants remove broad categories of speech – too swiftly for meaningful analysis.

Many countries have proposed or passed rules on these lines: Australia, France, UK, Germany, India. They are all bad, but Canada's is literally the worst – as if Trudeau's Liberals sought out the most dangerous elements of each rule and combined them."

Please implement this differently. I'm sure your intentions are good but this is a hamfisted and horrible implementation that seems designed to win votes than to actually solve a problem.

- Brad

From:	Donna Rivet (NELAC
To:	ICN / DCI (PCH)
Subject:	Censorship is government overreach and a violation of constitutional rights.
Date:	August 12, 2021 7:51:26 PM

To the Digital Citizen Initiative.

I am responding to your request for written submissions on the proposed approach to online harms. I would like to outline some concerns I have about the proposed approach, which will be ineffective at combating online harm and instead will capture non-criminal content and limit free expression.

The gravest danger of this proposal is that the government is setting up conditions that would favour government violations of Canadian Citizens constitutional rights, and provide a dangerous venue for government abuse. It is effectively a dismantling of democracy and creating Totalitarian policy. I don't recognize my country any more.

A government that seeks to control the narrative on any issue through censorship, is in effect, acting to create conditions that allow a government to limit citizen dissent. The very reason free speech exists in a democracy is so that government actions have a continual check. Without that, there is no democracy. Calling it a 'proposed approach to online harms' does not remove the violation to constitutional rights. "Trust us" is not good enough. There should be no policies or laws that open the door wide to potential, or even possible, government abuses of citizen's voices. That's why we have constitutional rights.

No one should have the power to control the narrative of the people's voices; not Big Tech, not Government, and certainly not a private corporation in partnership with government. Such conditions certainly should not be "necessary for a government's vision".

Mr. Trudeau is effectively acting as if the people's constitutional and charter rights no longer exist.

I'm increasingly alarmed at the complete lack of respect for the people's constitutional, and chartered rights that PM Trudeau is displaying.

We are increasingly seeing an overly close relationship of government and policy in line with Corporate interests. This is more than concerning. I

Mr Trudeau announced on National TV, that "Internet Censorship will be necessary for the government vision". This is a shocking statement in a democracy. This proposed approach to "online harms" is government overreach in the crudest manner. No politician has any legal right to dispense with fundamental rights in order to meet his particular 'vision' of government, and especially when that 'vision' increasingly involves violations of protected rights.

# Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

Nothing justifies the PM abdicating his oath of office which requires he protect the mation Act people's constitutional and charter rights, but to suggest that such violations are to continue as an arrangement by our government in partnership with Big Tech is outrageous.

Violations of those rights, as you know, are a grave matter. They are not 'given' to us by the current PM, nor can they be taken away by him. They can't be voted away, or traded. He acts as if he doesn't know this. Is this then, a display of current Liberal values?

The level of censorship and propaganda practiced already by Big Tech, is concerning. It was already an unacceptable situation that manipulation of public interaction online was happening at all by the tech companies. That governments asked for and sanctioned more of this sort of control in partnership with a private corporation is shocking. That it is being actively promoted by those who are under oath to protect our rights, is unacceptable. That such an extreme level of government control over Canadians free speech is presented as protecting the public from 'online harms' is a poor excuse for such an erosion of our constitution.

A partnership of our government with a private corporation involving restrictions on Freedom of Speech is highly questionable.

Just no. NO.

Sincerely,

Donna Rivet and Richard Rivet

Sent from my iPad

s.19(1)

From:	Star and Star and
To:	ICN / DCI (PCH)
Subject:	Stop Internet censorship
Date:	August 12, 2021 7:39:59 PM
Importance:	High
and a second second	_~~.

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act.

#### Dear Sir,

I am totally against the Liberal party's Bill to censor internet content. Canadians want their freedom, not more censorship. Stop this now!

Roman Rabenda

#### Felicia Mazzarello

From: Sent: To: Subject: Bert Iverson October 5, 2021 6:40 PM ICN / DCI (PCH) harmful content online -- proposals

s.19(1)

### About the proposed approach

The Government proposes a new legislative and regulatory framework that would create rules for how social media platforms and other online services must address harmful content. The framework sets out:

- which entities would be subject to the new rules;
- what types of harmful content would be regulated;
- new rules and obligations for regulated entities; and
- two new regulatory bodies and an Advisory Board to administer and oversee the new framework and enforce its rules and obligations.
- No way would I vote for any representative who advances these scary laws.
- Joan -- a Canadian citizen

 From:
 elena smith

 To:
 ICN / DCI (PCH)

 Subject:
 Attn: Digital Citizen Initiative

 Date:
 August 12, 2021 7:17:48 PM

I am writing regarding the proposed regulatory framework for "harmful online content". The proposed approach is most worrisome on a number of fronts in addition to which it will be ineffective at combating online harm. This is a limit on free expression.

I support efforts to remove criminal content from the internet, however, this approach will not achieve that goal and it dismisses concerns for fundamental rights of Canadians:

- the proposed 24-hour takedown requirement will lead to ill-considered (due to lack of time) removal of non-criminal content;
- the mandatory police reporting will result in use of AI (artificial intelligence) to monitor our speech and these records are very likely to include non-criminal speech. This noncriminal speech proactively being sent to police is an unsuitable and wasteful use of police resources;
- the proposed three new regulatory bodies is an enormous bureaucratic addition. The unreasonable powers to conduct broad inspections, including warrantless inspections reminds one of soviet officialdom. Freedom from unreasonable search must be respected;
- then further the Digital Recourse Council may conduct secret hearings. What extraordinary circumstances justify departure from the fundamental constitutional principles of "open court"?
- providing this regulator the power to block websites is simply government censorship.

This proposed Bill harms public confidence in and respect for the administration of justice.

Please make a new beginning and consider these issues.

Best regards, M. Elena Smith

From:	BRIAN BASTIEN
To:	ICN / DCI (PCH)
Subject:	Protect Free Legal Speech
Date:	August 12, 2021 7:15:18 PM

I cannot tell you how strongly I feel that our freedom of free legal speech must be protected. If any speech is legal then no one should be permitted to alter, censor, or disturb it. If anyone is permitted in any way to hinder free legal speech, then it creates the opportunity and incentive for those hindering speech to engage in nefarious practises that, for example advance their political and/or social objectives. If it's good enough to be said in the general media, then it should not be stopped in any way. One person's misinformation is simply a disagreement about it by another. Stopping speech on this basis is really giving in to those who do not want others hearing what they disagree with and dislike.

Sent from iPad

#### Felicia Mazzarello

From: Sent: To: Subject: Levo DeLellis October 5, 2021 11:04 AM ICN / DCI (PCH) Harmful Online Content

s.19(1)

Hello I am reading about the harmful online content proposal <u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html</u> In the technical paper here <u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-</u> <u>content/discussion-guide.html</u>

Under "Module 1(B): New rules and obligations" "General obligations" it makes mention automatically decision making may be required. As someone who writes code and logic that may be used for this I absolutely hate this and do not support this proposal as it is written. I seen too many instances where this was applied and 100% of the time it causes problems. The only time it seems reasonable is when it did nothing but insert a warning

I'd be more comfortable when the following alternatives

- Warnings were added to suspicious content

 Advisories on strange groups such as flat eathers and anti vax. Perhaps a learn more link which informs users about "Russian troll farms" and that members of the group may not believe anything they're saying but intend to cause disruption in their lives

- Having sites informing users how many hours they spend and suggest to take breaks or warnings that what they see may be misleading or promotional content

But nothing that prevents anyone from doing anything or automatically report/flag anyone (I can explain why if you wish). Absolutely nothing should mix automation with reporting or impeding someone from doing anything

 From:
 Shari Friesen

 To:
 ICN / DCI (PCH)

 Subject:
 Censorship

 Date:
 August 12, 2021 7:11:51 PM

Canada will start becoming a communist country if we allow our government to put restrictions on our rights. This includes vaccine passports as well. Our government needs to STOP taking the rights of Canadian citizens away.

#### Felicia Mazzarello

From: Sent: To: Subject: Olivier Bourque October 5, 2021 10:29 PM ICN / DCI (PCH) Huawei et contenu préjudiciable en ligne

s.19(1)

Madame, Monsieur,

Le but premier de ce message est de vous dire que je suis fortement en accord avec le ban de Huawei en sol Canadien. La raison principale est que le gouvernement Chinois n'est tout simplement pas digne de confiance. Le Parti Communiste de Chine nous prouve depuis longtemps que ses ambitions totalitaires se manifestent par la perte de droits humains fondamentaux. Les gens informés savent que les compagnies chinoises volent depuis longtemps les propriétés intellectuelles de nos compagnies et de nos universités à travers ses investissements, échanges étudiants, piratage informatique, etc... Quand on sait en plus que le peuple Chinois est soumis à des contrôles comme la reconnaissance faciale combinée à un système de crédit social avec comme but final de punir les esprits libres et les détracteurs du Parti. Ce n'est vraiment pas une vision de l'avenir de la race humaine que j'aime envisager...

Huawei devrait être adressée par le NATO. Pas de technologies Russe, Chinoise, (ou autres dictatures) dans aucunes de nos infrastructures clés.

Deuxièmement, je voulais faire part de mon fort désaccord avec l'approche proposée du gouvernement pour s'attaquer au contenu préjudiciable en ligne. Pas que le message principal soit mauvais. Qui de censé ne voudrait pas un Internet sans pornographie juvénile, terrorisme, discours de haine, etc...? Les raisons principales de mon désaccord sont la méthode qui sera utilisée pour gérer le contenu et les personnes qui déciderons du contenu sensible. Twitter, Facebook, Google ont déjà commencé avec leurs IA. Les intelligences artificielles ne font aucunes distinctions, elles suivent un code. Mais qui décide du code? Au début, on nous dira que c'est pour "protéger les enfants et les minorités" et ensuite il y aura des amendements. On inclura peut-être des anti-vaccins, des conspirationnistes, des formes de satire, etc... Je crois pour ma part qu'il faut laisser les gens s'exprimer et former leurs propres opinions. Quitte à risquer être témoin de ce contenu sensible. Vraisemblablement, la meilleure méthode pour contrôler l'Internet est la méthode Chinoise. Comme je l'ai décrit plus haut, cela veut dire une absence de liberté et d'autonomie.

Internet est un besoin essentiel, il faut laisser les provinces nationaliser les télécoms.

Salutations, Olivier Bourque

 From:
 MF GM

 To:
 ICN / DCI (PCH)

 Subject:
 Online version censorship

 Date:
 August 12, 2021 7:04:07 PM

I don't know anyone who thinks government censoring free speech online is a good idea.

You will never be able to define hate making the legislation impossible to follow. It will flood courts with frivolous claims. You will look like the evil empire. Let people decide what they want to watch and not watch. It's really that simple. In fact, i can't think of anything More unCanadian than censoring free speech.

 From:
 Richard Killy

 To:
 ICN / DCI (PCH)

 Date:
 August 12, 2021 6:51:07 PM

The proposed legislation that would seriously curtail freedom of speech under the promise of reducing harm. Is nothing but censorship.

Hurt feelings isn't a crime. I've had my feelings hurt my whole life, but that doesn't make that a crime, or those that did it criminals. Nor should those same people be singled out by this legislation. IOnly things that are criminal offences should ever be restricted, not points of view.

This legislation is the governments way of controlling our right to express an opinion. If 1 don't like someone's opinion, I ignore it. But 1 don't want legislation to stop others from expressing that opinion.

Richard Killy Canadian Voter and Tax Payer

From: To: Subject: Date: schmotta schmotta ICN / DCI (PCH) Ministry Heritage InternetLanguage posting Policed -Free Speech August 12, 2021 6:43:06 PM

#### COMMENT:

# Freedom of Speech is integral to a free and democratic society.

## Canadian citizens DO NOT WANT INTERNET LANGUAGE GESTAPO.

I am thoroughly repelled by the marxist liberal party who behave in such a condescending paternal manner. YOU ARE NOT "DADDY". STAY OUT OF OUR LIVES! If you don't like what a person has to say- don't read it. I STAND FOR FREE SPEECH AND ACCOUNTABILITY AND RESPONSIBLE BEHAVIOUR IN SOCIETY. A FREE SOCIETY! FREEDOM!!!

Canada is a fake government because Canada is Canada Inc. and masquerading as a government.

#### DO NOT POLICE THE INTERNET.

The election could not come sooner.

Justin Trudeau & his cabinet will stand trial for crimes against humanity under Nuremberg code violations for his heinous role in the covid-19 "Event 201" live exercise and simulation FRAUD. There is no Sars-Cov-2 virus.- Hence, all health mandates based on this virus are fraud and vaccines could never be made without a piece of the actual virus. Canadians were not informed of the experiment nor given the inoculation leaky gene therapy contents. The entire plandemic is a psyops- no matter how he attempts to control the crime and to attack truthers & white hat physicians/nurses who are in every hospital in this country ready to give evidence despite being threatened and intimidated by fake government thugs.

## **STAY OUT OF OUR LIVES.**

To: Subject: Date:	ICN / DCI (PCH) Comments on "The Government's proposed approach to address harmful content online" August 12, 2021 6:29:38 PM
From:	Document released pursuant to the Access to Information Act.
s.19(1)	la Loi sur l'accès à l'information.

I recently read about the proposal for an Act of Parliament to "address harmful content online", and was very disturbed by how poorly-conceived the plan is. I'm very aware of the threat that violent extremism poses online, but the proposed plan is a massive overreach that will greatly limit Canadians' free expression in other ways, and on top of that will most likely be ineffective at its intended purpose.

The massive penalties and onerous requirements on ISPs, websites, and the like will most likely lead to them instituting overly broad censorship policies to avoid falling afoul of the law. Also, actual right-wing extremists often abuse reporting systems like this one to effectively censor those who speak out against them. Finally, the overly broad scope of the Act means that the law enforcement body reviewing reports will have to waste its time with huge numbers of false or spurious reports rather than dealing with actual harmful content.

I urge the government to reject the proposed Act and reconsider their approach.

#### Felicia Mazzarello

From: Sent: To: Subject: Kirk Fast < October 21, 2021 10:04 PM s.19(1) ICN / DCI (PCH) I reject the scope of the harmful content proposal

Most of this is a form letter, but putting in my 2 cents to start. Policies like the one being proposed only serve to limit peoples ability to speak freely. There is room to create a policy around limiting items your are proposing, but it can't be at the expense of our ability to speak our minds. Tighter controls on what can be looked at, how it will be interpreted, how people can appeal, and consequences for false reports must be included in any laws put together. I know some of these things are in the proposal, but from what I've looked over, they are vague to the extent of "a body will deal with it", which is too generic.

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Kirk Fast

Giocommit commonique en virral de la Lao avercanada à l'Information Distancent information des la composit fo the viccosa la minamanistrate

#### To Whom It May Concern,

I would like to take a moment to say that I do not approve of additional censorship of the internet. I believe that it is a form of terrorism to try and control freedom of speech. As a concerned Canadian Citizen, I have always been proud to live in a country that stands for the freedom of its people as listed in our "Canadian Charter of Rights and Freedoms" which states:

Everyone has the following fundamental freedoms:

(a) freedom of conscience and religion;

(b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;

(c) freedom of peaceful assembly; and

(d) freedom of association.

Thank you, Dawna Weber

 From:
 Paul Jenkins

 To:
 ICN / DCI (PCH)

 Subject:
 "Online harms" and legislative overreach

 Date:
 August 12, 2021 6:17:20 PM

While online harms can indeed be egregious, proposed legislation to regulate and censor online speech is on a slippery slope to tyranny. Robust conversation and debate are the only effective ways to untangle disputes and avoid dangerous polarization. When the free exchange of ideas is suppressed, dangerous conditions arise and samizdat in some form will emerge. Truth must eventually win the day.

Paul Jenkins

Cydnee McCloud
ICN / DCI (PCH)
Against the proposed approach to control harmful content online
August 12, 2021 6:13:48 PM

Good afternoon, I am writing to you to voice my opinion that is against the proposed approach to control harmful content online. The proposal is a ludicrous violation of free speech and will only serve to make the internet a place where Canadians can only view the most milquetoast opinions. People will be afraid to say anything for fear of getting their account suspended or banned. Companies and websites have zero incentive to actually do any kind of work identifying speech that is actually harmful to minors or minorities, and will simply block a post or a user and never bother to check to see whether it's actually harmful. Even if an appeal is submitted, they're under no obligation to review the content in question. This is also extremely harmful for lawful, consensual sex workers. This proposal needs a major overhaul, if not just be scrapped entirely and started from scratch. It takes the worst parts of laws other countries have tried to pass. We need to be better than that.

Sincerely, Cydnee McCloud

 From:
 Anna Dupas

 To:
 ICN / DCI (PCH)

 Subject:
 Free speech

 Date:
 August 12, 2021 6:00:12 PM

I am writing to protest in the strongest possible terms your government's intention to restrict free speech. You couch it in terms such as 'restricting hate speech,' but that's pure BS and you know it. I was banned on Facebook for a month because I rightly called our current joke of a PM a 'dictator.' So now in Canada we can't even criticize our government leaders? I guess we're living in Communist China or North Korea now, and your proposals will only make it worse. Your government has been nothing but poison to Canada. The sooner you're out, the better. You're nothing but a Crime Minister, and you're the worst leader Canada has ever had.

Sent from

s.19(1)

#### Felicia Mazzarello

From: Sent: To: Subject: Ryan Ross < September 26, 2021 8:16 AM ICN / DCI (PCH) Internet censorship bill

s.19(1)

To whom it may concern,

I am writing to you regarding the proposed Internet censorship bill

Harmful content is a real problem online, and careful legislation could help reduce its prevalence without stamping on our rights. But the proposal set forth in the consultation is SO FAR from the nuance we require that it would make Canada the most CENSORED democratic country in the world.

This draft proposal is anything but careful. It's an unprecedented expansion of law enforcement surveillance of lawful online speech, and will force online platforms to remove many forms of lawful and socially important activism and speech.

I and most Canadians believe deeply in freedom of expression. We Canadians have often defended everyone's ability to access and express themselves freely on an open Internet in Canada and around the world.

To lose that freedom would be a huge loss.

Sincerely,

Ryan Ross

Sent from my iPhone

From:	Ariana McKone
To:	ICN / DCI (PCH)
Subject:	Bill C-36
Date:	August 12, 2021 5:47:25 PM

Dear Sir Or Madam,

I hope this email finds you well.

I am writing to you today to express my deep concern about Bill C-36. As we already have laws against acts of hate that apply to in person as well as online actions, This proposed law seems directed not towards protecting people against death threats or from calls to violence but instead as a way for one group of people with a certain view to silence any opposing views. Any time the government takes steps towards in acting laws that determining what can be said in public, we are running towards a totalitarian state. No perceived good that can come from such a law will come even close to the harm our nation will face as a few people sit in judgement as arbitrators of truth. The danger all freedom faces when people can anonymously accuse anyone of a "crime" and bear no responsibility for making the accusation, While the accused will have to spend 10's of thousands of dollars defending themselves, not against the person who accuses them, but against the government with unlimited resources knows no limits.

I think Ralph Waldo Emerson sums it up well, He says

"Let me never fall into the vulgar mistake of dreaming that I am persecuted whenever I am contradicted."

For these reasons I am asking you to reject B C-36 in its entirety. Respectfully,

Ariana McKone

s.19(1)

#### Felicia Mazzarello

From: Sent: To: Subject: G -October 4, 2021 12:41 PM ICN / DCI (PCH) Internet regulation

s.19(1)

Hi

I am very concerned about the damaging content that is online and available to youth and children.

Youth and children have never been exposed to pornography and hateful content and violence like today because of the internet. To date nothing has been done to stop this

We are essentially destroying and ruining the innocence of our children and youth because online pornography and hateful and violent content is so readily available to our children and youth on the internet. So many youth are being harmed by this content and their innocence is being destroyed. This needs to be addressed and stopped

As the ministry responsible for protecting our youth from harmful content your government has not done anything to stop this. I dont believe the new bill C-10 does anything to regulate pornographic or hateful websites so that children cannot view it ?

Could you please tell me what you plan to do to to protect youth from pornography sites and hateful websites ??

When a child or youth goes to a physical store they have to be 18 or over to purchase any type of adult content or pornography. Why is that we dont do that on the internet. Any site that has adult content must ensure that only adults are able to view it or have some sort of registration where they ensure the user is over 18 ??

Same with websites that have hateful or violent content ?

Could you please respond specifically to this issue and what you will do to stop this

Thanks Gord

From:	Valerie Lafrance
To:	ICN / DCI (PCH)
Subject:	Absolute NO to additional censorship
Date:	August 12, 2021 5:41:06 PM

Hello,

I formerly and clearly request that the canadian government not add any more censorship laws or regulations. In fact, much too much content is already censored when it shouldn't be, and there should be a motion to reduce censorship in Canada and protect freedom of speech.

Respectfully,

Valerie Lafrance

From:	Read Red
To:	ICN / DCI (PCH)
Subject:	Internet censorship
Date:	August 12, 2021 5:40:06 PM

#### To whom it may concern,

Early on in the covid 19 pandemic, it became clear that there was little tolerance for dissenting voices with regard to pandemic response dogma, ie; lockdowns, masking, and now the mass vaccination campaign. We were constantly told to trust the science, but when credible doctors and scientists disagreed with the aforementioned public health mandates they were met with censorship on popular social media platforms like Twitter, Facebook, and YouTube etc. We saw an intolerance for dissent and public discourse become normalized. In my opinion, this kind of precedent, where we silence doctors, scientists, academics, politicians, citizens, is far more scary than a nasty respiratory disease, because the virus will run its course, but the changes we make as a society, heavily regulated internet, a vaccine passport, these are knee jerk decisions born out of fear, and we'll be stuck with these changes for years to come, and we will have lost a part of who we were, an important part. We should allow for robust public discourse on such measures, and perhaps even make them subject to a voting process, that's how important I believe these decisions are. In normal times we are proud of our western democratic freedoms. Internet censorship, heavy regulation in the wrong hands, is a move toward something resembling authoritarianism. Censoring disagreable opinions doesn't make them go away. Kicking racists off of social media, though I understand the temptation, does not solve racism. I prefer a society where we challenge ideas with intelligence and compassion, even dangerous ones, not run from them or lock them in the basement. That's who I think we are.

Thanks for your time, MW (

s.19(1)

RED

000920

 From:
 John Toogood

 To:
 ICN / DCI (PCH)

 Subject:
 Online content consultation

 Date:
 August 12, 2021 5:38:43 PM

The Government of Canada has requested feedback on its proposals to regulate online content.

My feedback is that the correct form of government regulation of online content is absolutely no regulation whatsoever, apart from enforcement of existing law. Therefore, my view on the proposals in your consultation paper could be concisely summarized as "no".

Thank you very much for requesting feedback.

John Toogood

s.19(1)

From:	connie	
To:	ICN / DCI (PCH)	
Subject:	RE CENSORSHIP	
Date:	August 12, 2021 5:38:22 PM	

It is unconstitutional and illegal to censor information as this is an infringement on people's freedom of speech and freedom of information.

s.19(1)

It is also a conflict of interest for the Liberal government to fund (bailout) the mainstream media with taxpayers' money and then control the content they put out by only allowing a biased narrative.

Canada is supposed to be a democratic country however, the tyranny and overreach of the government have gone too far and I honestly don't know why government officials have not been arrested for treason as of yet.

I support freedom for all Canadians!

I stand by the Charter of Rights and Freedoms!!

Connie

#### Felicia Mazzarello

From: Sent: To: Subject: Carson Bishop October 5, 2021 5:35 PM ICN / DCI (PCH) Legislation of Online Harm

s.19(1)

Hello,

Do I really need to explain why this is a terrible idea. The privacy concerns, the thought of who says what is hate speech, it won't always be the liberals on charge. The idea that social media platforms won't start removing and banning any controversial content to avoid fines. Horrible idea unless your ultimate goal is censorship and the inability to communicate with one another about real issues.

Cheers,

Carson

 From:
 Monieca S

 To:
 ICN / DCI (PCH)

 Subject:
 Censorship

 Date:
 August 12, 2021 5:36:43 PM

What you are proposing is against our right to freedom of speech and a harmful and unlawful! This is so anti Canadian I am shocked! Shame on you!

Your time and resources will be better spent going after pedophiles, drug dealers, human traffickers and other real criminals.

Sent from my iPad

 From:
 Gene Goodreau

 To:
 ICN / DCI (PCH)

 Subject:
 Online Speech Regulation Proposal

 Date:
 August 12, 2021 5:31:42 PM

#### DO NOT REGULATE THE INTERNET!

I do not agree with any form of internet content regulation.

Thank you,

Gene Goodreau

#### Felicia Mazzarello

From: Sent: To: Subject: Magda Zaplotny, RCIC September 28, 2021 7:22 PM ICN / DCI (PCH) Magda

s.19(1)

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Magda Zaplotny, RCIC

optimus prime
ICN / DCI (PCH)
Re: Online Harms Consultation
August 12, 2021 5:12:17 PM

Hello, I am writing to you today to express my concerns with the governments proposed approach to address online harms.

The governments proposals are a mashup of some of the worst ideas around the world that have the potential to cause massive collateral damage to freedom of expression online. These include:

·broad definitions speech that is legal but may be harmful and it's mandatory reporting

•takedown requirements that are too short to throughly review and consider context or nuance of speech

• an effective filtering requirement that will cause many false positives as the sheer size of the internet will require robots that cannot understand context or nuance to work

•website blocking of sites that have violated the proposed requirements too many times, which I believe should never happen

These actions have proven to cause problems in other countries around the world that have implemented them or similar requirements that affect the most marginalized communities most such as automatic removal of police brutality and human rights violations or preventing racialized people from sharing the harmful messages they receive. These proposals will also embolden authoritarian countries to introduce laws that further repress their populations.

None of these proposals should be implemented as they will only do more harm then good and sweeping truly harmful speech under the rug rather than address it. Sincerely, Brennan

Sent from my iPhone

 From:
 Joshua Morton

 To:
 ICN / DCI (PCH)
 S

 Subject:
 Do Not Approve New Online Controls
 S

 Date:
 August 12, 2021 4:34:21 PM
 S

s.19(1)

I am a citizen of Canada living and I am against the approval and implementation of the new proposal to control online services and content. The planned approach will give far too great a power to the 'Digital Safety Commission of Canada' that would allow them to threaten and harass smaller online service providers, while giving them protection should they use their powers to promote their own personal agendas or work against the efforts of other organizations. The Commission would simply have too much power and too few safeguards, especially concerning their ability to conduct activities out of the public eye.

The proposal also favours large, highly wealthy corporations such as Facebook, Twitter, Microsoft etc. by potentially forcing online service providers to conform to regulations that would drastically increase their operating costs. Smaller companies who cannot afford to implement features such as algorithmic moderation or data tracking on a mass scale would be eliminated, giving greater dominance to these larger corporations who already control the majority of online services and content.

These new rules would also work against the right to freedom of speech for the average citizen. Though the proposal promises to ensure online content that is harmful is removed, it does not account for situations where content is removed yet proven to be safe. Companies and individuals will be punished for creating and promoting harmful content, yet will these companies be punished for removing safe content? Where are the regulations for that situation? Under this plan, online service providers would be encouraged to remove any content that has any possibility of being harmful very quickly, yet face inadequate penalties for removing safe content. Therefore, they can remove content with impunity. This will likely lead to a situation where moderation is lax, providers will simply remove anything with any hints of being harmful. Open discussion will be shuttered and Canadian citizens will find the content they can create and explore to be heavily restricted.

For this reasons and others, I am against these new proposals. This is not the way to reduce harmful content or to control and police online services.

Joshua Morton

Ethan Evenson
ICN / DCI (PCH)
Harmful Content Comment
August 12, 2021 4:14:26 PM

This proposal is absolute lunacy, and it infuriates me that such an incredibly important policy was largely hidden from the public for so long. Obviously this wasn't exactly hushed up, but much like a number of recent proposed pieces of legislation, I've had to dig for a while to find it.

Any and all parts of this proposal are detrimental or wastes of time. Creating additional agencies that have no economic benefit then staffing them with idealogues is a fantastic way to waste even more money for no return, when our budget should be concentrated elsewhere, especially for the native community right now. Cutting Canada off from the rest of the internet by forcing overseas sites to implement our policies is going to slow our progress and remove us from global dialogues, and to an extent, trade, as some companies might not see the point in having localized Canadian versions of their services, preventing private individuals from making exchanges and purchases. "Stopping extremism," or any such statements is pushing for extremism on another front, of government control, and against the rights of the individuals. This is something that Canadians would massively oppose if it were more public and visible, instead of something they need to dig for, then give away their identity to make comments on.

The government should not go through with any of this.

 From:
 William Steele

 To:
 ICN / DCI (PCH)

 Subject:
 Digital Citizen Initiative - Harmful Content Response

 Date:
 August 12, 2021 2:59:17 PM

Digital Citizen Initiative,

As I'm sure that you are currently working with a lot in this swift-moving proposal for alleged "digital safety", I will keep this as concise as possible.

The proposed approach as outlined in a technical paper and discussion guide, currently provided on the Government of Canada's website, is frankly not at an acceptable level to be written into law with the potential to do irreparable harm to Canadian citizens and their constitutional rights.

" 11. [A] The Act should provide that an OCSP must address all content that is flagged by any person in Canada as harmful content, expeditiously after the content has been flagged.
[B] The Act should provide that for part [A], "expeditiously" is to be defined as twenty-four (24) hours from the content being flagged, or such other period of time as may be prescribed by the Governor in Council through regulations."

A window of 24 hours to appeal to flagged content is too short to have any fair and sensible justice to be enacted, and the reporting of falsely flagged content by those who would eagerly abuse a reporting system in order to censor content.

#### "Module 1(A):

The Act should would be based on the following premises:

Recognize the many benefits that Online Communication Services (OCSs) bring to Canadian society, such as facilitating communication with friends and family and participation in public discourse, enabling companies to reach domestic and foreign markets, and providing space for activists, organizations, and civil society to organize and share their messages;

Recognize that OCSs can be used as a tool to spread harmful content;

Consider that the hatred spread online often has a disproportionate impact on women, Indigenous Peoples, members of racialized and religious minority communities and on LGBTQ2 and genderdiverse communities and persons with disabilities;

Consider that OCSs are used to spread propaganda, recruit, organize and incite violence, and that terrorist content online often leads to violence in the physical world;

Consider that OCSs are used to share content depicting real-world acts of violence in an effort to incite violence, intimidate the public or segments of the public, and damage societal cohesion; Consider that OCSs are used to sexually exploit children online, and that such exploitation can have life-long consequences for victims;

Consider that OCSs are used to share the sexual content of others without their consent, resulting in life-long consequences including re-victimization; and

Respect and protect the ability of peoples in Canada to fully participate in public discourse free from harm, while protecting fundamental freedoms and human rights."

#### Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

This is especially dangerous to the rights of vulnerable groups such as Black people, Indigenous after Active people, People of Colour, LGBTQIA2S, as well as those who exercise their right to vocal disagreement, protest and discussion. The definition of "terrorist/terrorism" is both vague and exploitable in the silencing of peaceful protests and the concerns of marginalized communities raised towards governmental authority.

Furthermore, any abuses of this Act towards protesting marginalized groups cause the modular act to fail in its own established premises, creating a heavily-monitored experience where fear of extreme punishment prevents freedom of speech and discussion in the betterment of governmental process and implementation.

A system that uses "automated systems" to flag content without awareness for subtleties in human interaction, nor awareness for communicative context cannot be trusted to make such impactful allegations against Canadian citizens.

Canadian citizens currently live in a time where abuses of police are already made more public and incompetency within government bodies cause citizens to lose trust in said bodies. Your current proposal is hastily and clumsily rendered at best and potentially draconian in practice at worst.

I hope that you would be able to review, revise and potentially rescind your current proposal in favour of consultation with more digital experts and community leaders to ensure the safety and freedom of Canadian citizens. Going from a consulted platform, you might be able to find more effective ways to combat child exploitation and properly use hate-crime laws to defend the vulnerable people of Canada rather than (knowingly or unknowingly) attack them.

Thank you for your time,

s.19(1)

William M. Steele

 From:
 Steven Houle

 To:
 ICN / DCI (PCH)

 Subject:
 Censorship breeds paranola and martyrdom.

 Date:
 August 12, 2021 2:56:33 PM

I strongly oppose any sort of online censorship bill. The items that were proposed are already illegal and those who break those laws ought to be persecuted over them. I historically voted liberal, but with this strong arming of bills being pushed through in attempt again and again they lost my vote.

While I agree that anti-vaxx and disinformation campaigns are harmful, it is a necessary evil to allow for development of thought and discussion. Sunlight is the best disinfectant, having people post these comments under their full name on Facebook is a lot easier to find and, if illegal content is found, persecute than to have them go on anonymous underbelly forums. Being able to hear Jordan Peterson prattle on for 3 hours in a Joe Rogan podcast does more to show how dumb and illogical his theories are than seeing his posts banned on social media with only blurbs in articles about it. There's a saying, give enough rope and watch them hang themselves with it.

Having such laws in place will easily become a hammer solution where the company oversteps the mandate and just stagnate all discussion. The conspiracy theorists who are already predisposed to bs will find and share their views on more insidious websites while those who would otherwise be exposed to the full debate and debunked conclusion. What happens then? Start having government IP bans? Sounds a lot like something what our big three media companies have been lobbying for. This legislation is so easy to hijack and use in a more broad sense. Let's not become like other countries that have such anti freedom of speech measures. Let's not join the ranks of China.

When you censor discussion it grants legitimacy to the eyes of the paranoid mind. "this is the information that THEY don't want you to see". It is also easy to bypass censorship. If teens on TikTok can bypass china censors with character inserts and older person can on Twitter. I used to be a moderator on a popular social media website and when there are banned words or discussion it quickly becomes codified into something else. 'Ninja', and 'Roys' come to mind from those days. Can you guess what they are used to mask? If not this demonstrates such simple measures as to why censorship does not work - especially from an algorithmic sense. Just look at the growing pains Tumblr went through when its algorithm was used for nudity. You not only don't censor discussion but then give people a second thought of "what is it that they don't want us to see that is worse than what we see in a book, or documentary".

It is difficult to discuss this without bringing up 1984, Minority Report, hell - even Metal Gear Solid. It goes to show just how short sighted and immature such legislation is when old media from multiple sources of media have already explored the topic for entertainment. We as a society have the responsibility to challenge lies, challenge troll farms and disinformation campaigns, and challenge the belligerence and disregard that some people show towards the safety of our fellow Canadian.

This email may be jumping around a bit but I hope that this expresses my strong dislike for any sort of government censorship legislation, especially for those who do not understand the internet. I was prompted to post this from seeing information that ,despite the overwhelming negative reaction that the recent bills received, that this is still going on.

#### Felicia Mazzarello

From: Sent: To: Subject: Elizabeth Burrows < September 30, 2021 8:56 AM ICN / DCI (PCH) ON

s.19(1)

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Elizabeth Burrows

Kuni Zyrekal (DE .4)
ICN / DCI (PCH)
The Government's proposed approach to address harmful content online
August 12, 2021 2:19:54 PM

You have taken the worst parts of other countries' attempts at Internet censorship, and made something worse.

The fact of the matter is, hate speech, revenge porn, and child porn are already illegal. Utilize the existing laws. The proposed changes are draconian and poorly defined. Companies will comply by being overly cautious and in turn stifle freedom of expression. 24-hour turnarounds are quite frankly, insane. The end point of that is no checking of the complaint and instead automated takedowns.

While the intent is good, the execution is deeply flawed. Please take notes on why the proposed laws in other countries have been struck down. That does not mean try again but even harder, it means take a new approach, one that does not harm innocents. I agree that the proposed 5 sections are bad, and actions should be taken, the fact of the matter is that this will have unintended consequences.

As someone who produces, and is friends with people who produce, what some people would describe as obscene content, I fear this is simply the stepping stone to removing our content and livelihood. Please, listen to people who work in the sex entertainment industry and work with them. None of us want children harmed, nor revenge porn to exist, but laws need to be made that include safe harbour for those of us producing legal porn. The proposed law is dangerous to us, and onerous to companies.

From:	Julien Paquette
To:	ICN / DCI (PCH)
Subject:	Awful initiative
Date:	August 12, 2021 1:33:38 PM

I really don't have the words that can quite describe how I feel.

Hell is paved with good intentions fits this perfectly.

There are many things wrong with social media, and companies have showed time and time again that they cannot handle or mediate the beasts they've created, and social media are breeding grounds of harmful content, and there are initiatives that could help. But not this.

I don't understand how the Liberal Party can look at similar laws in other countries, see their flaws and failures, and actively seek out the **\*worst\*** parts of them and say « Yes, that's what we need ».

I do not have the energy to go through all the things that is wrong with it, but here are some key points :

-The speed at which the system detects content and demands its removal is **\*way**\* too fast for a proper, contextual analysis. Militants and Human Rights Activists are just as much at risk of censorship as those who actually share harmful and violent content.

-Leaving the initiative open to let any future governments to add and remove what content should be regulated is **\*beyond asinine**\*. This paves a passive way for autocrats and bigots – which the Canadian Government isn't free of, let's face it – to change the régulations to what fits them bests. There are reports of Alberta using a similar « misinformation filter » to remove any anti-oil/pipeline content from social media, and Following the very recent Climate Change Report, I think it's safe to say that this behaviour is worrying.

Please reconsider. This is alarming,

Sent from Mail for Windows

 From:
 academicalism
 I/ICE

 To:
 ICN / DCI (PCH)
 I/ICE

 Subject:
 Rethink—or scrap—unconstitutional "online harmful content" proposal
 Date:

 Date:
 August 12, 2021 12:04:40 PM
 PM

Dear members of the Canadian government's "Digital Citizen Initiative,"

I am writing to express my alarm and disapproval over the proposed online harms rules the Canadian government now proposes—a combination, it seems, of the worst, most rights-violating regulations adopted in other jurisdictions, many of which (like China) aren't exactly known as bastions of democracy and expressive freedoms.

Your proposal's combination of

- \* prohibitions of broad and poorly defined speech categories;
- \* disproportionate penalties for insufficient blocking; and
- \* requirement of rapid compliance without time for adequate assessment or counter-notifications

all guarantee that the major tech firms, on which the onus of your proposed regulations falls, will block all kinds of legitimate speech— and will disproportionately affect marginalized and minorities to persons and communities, as has been shown where such rules have been implemented elsewhere. Online harms rules have proven a human rights disaster in other jurisdictions; France's rules were recently ruled as unconstitutional.

I urge you to take this whole proposal either back to the proverbial drawing board—or entirely off the table. The Canadian government surely has bigger and more urgent priorities then over-regulating and preferentially censoring citizens' constitutional expressive rights and freedoms.

Sincerely

Mark A. McCutcheon
Professor, Literary Studies
Chair, Centre for Humanities
Athabasca University
1 University Drive
Athabasca, AB T9S 3A3
1-833-850-8202

 From:
 Steven Greenbank

 To:
 ICN / DCI (PCH)

 Subject:
 Online Harms

 Date:
 August 12, 2021 12:04:32 PM

The current government is set to destroy the internet and silence marginalized communities with its online harms legislation.

They will only serve to entrench the authority of tech giants, who are the only ones who could meet the demands of this legislation, to overpolice users, who will then be sent to law enforcement agencies that will, as they have always done, mistreat marginalized users faced with spurious complaints.

The government should abandon this legislation. And they should do it today!

## Felicia Mazzarello

From: Sent: To: Subject: Yu Dong November 5, 2021 9:00 PM ICN / DCI (PCH) Re: Online Harm Bill

s.19(1)

nigger nigger nigger nigger nigger nigger

fuck you

kill yourself

slit your wrists

hang yourself

drop a toaster in your bathtub

put a gun to your head and pull the trigger

censor this faggot

From: Yu Dong Sent: Friday, November 5, 2021 8:55 PM To: pch.icn-dci.pch@canada.ca <pch.icn-dci.pch@canada.ca> Subject: Online Harm Bill

Stop trying to censor the internet you disgusting piece of shit, I hope you die.

From:	Rebecca Hummel
To:	ICN / DCI (PCH)
Subject:	Online Content Moderation comment
Date:	August 12, 2021 11:46:53 AM

Though the objectives are noble, the proposed measures to be taken against harmful online content veer into undemocratic territory.

With massive fees and broad restrictions, most if not all online communications services will lean into the easiest and safest censorship algorithms. Though the proposed Act claims to value freedom of expression, debate, and information in an online space, it will create an environment where the platforms themselves are pressured into excessive censorship.

For example, the 24-hour window to address reported content is much too short for nuanced interpretation of the content and its context. The content is more than likely to be completely hidden from Canadian users, regardless of what it actually is. It could be educational, or news that addresses harmful content in an informative matter. It could be anything and OCSs, intimidated by the fines, will certainly automate the removal process entirely.

All Canadians could be withheld from the very information they need to educate themselves on the problems faced by the people who are the most harmed online, and Canadians who are marginalised or victimised could be withheld from resources or even the terminology to get help. No algorithm could grasp every possibility or nuance of online communication and could very well cause as much harm as they solve.

Hateful individuals and groups can be creative in how they circumvent automated moderation, or moderation done by real people who are put under exorbitant pressure of large quantities of reports that must be dealt with in such a short time frame. Even with these proposed measures, harmful content will persist.

Of additional concern is the matter of the Digital Safety Commissioner and the Digital Resource Council. Putting the onus of judging online content on so few (with the most power going to the Commissioner, a single person) provides a frightening opportunity for one person's biases and political agendas to reshape the internet most Canadians use to educate themselves and keep up with current events. There is no telling what a future Digital Safety Commissioner will deem harmful or for what reason, and the results of their decision will affect millions. Such power should not be given to a single person.

With the vastness of social media and the ever-growing presence it has in the lives of most Canadians, digital safety is not something that can be taken lightly. The harm it causes should be addressed as well as possible without trading it for undemocratic censorship. The proposed Act as it is now would have harmful, restrictive repercussions beyond what is plainly written in the documentation.

Thank you for your time and consideration.

 From:
 Randy Klein

 To:
 ICN / DCI (PCH)

 Cc:
 carolyn.bennett@parl.gc.ca

 Subject:
 Proposed Online Harms Legislation

 Date:
 August 12, 2021 10:37:26 AM

s.19(1)

To Whom It May Concern.

as someone who's participated in content moderation, and as an advocate of a competitive and mee market for on-line discourse, I am registering my opposition to this misguided legislation. The proposed law is: over-broad and vague in defining harmful speech categories; allows room for arbitrary and/or politically motivated changes by subsequent governments; imposes harsh penalties and rushed compliance deadlines that will end up favouring large incumbent monopolists while unfairly penalising small competitors and marginalised content creators; and uses technological "solutions" such as the creation of a Chinese-style national firewall and reliance on highly flawed and biased machine-learning algorithms (instead of properly trained and compensated humans) to police content.

Harmful but legal speech on the Internet is a serious problem. The most effective way to address it is by taking anti-trust action against the major social media platforms (most prominently Facebook and Twitter) that have thus far shown little interest in policing truly harmful and hateful content that spreads virally in their "walled garden" ecosystems. The most effective way the government of Canada can take action in this regard is the require that any social media platform operating in the country must allow (via open APIs and Internet standards) for interoperability with competitors and new entrants into the market. This will in turn promote the concept of federated messaging/social media services, which tend to be more effective and flexible at reducing the spread of harmful content (see, e.g. the case of the right-wing-populist forum Gab once it moved to the Mastadon platform:

https://www.theverge.com/2019/7/12/20691957/mastodon-decentralized-social-network-gab-migration-fediverse-app-blocking).

Before pursuing this matter further, I would urge you to read the following critiques of it by recognised experts Michael Geist (<u>https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/</u>) and Cory Doctorow (<u>https://pluralistic.net/2021/08/11/the-canada-variant/#no-canada</u>), whose writings alerted me to this issue. I am also copying this e-mail to my MP, Dr. Carolyn Bennett, and would appreciate her response as well. Thank you for your consideration and time.

R. Klein

From:	Alexander Saxton
To:	ICN / DCI (PCH)
Subject:	Harmful content legislation
Date:	August 12, 2021 9:51:41 AM

To whom it may concern,

I'm writing to express my vigorous opposition to the government's proposed legislation on harmful online content.

I think the legislation will be disaster for Canadians engaged in legitimate speech and expression, and that the bill's most disastrous consequences will be shouldered by those who are already most marginalized: people like sex workers, indigenous activists, and those engaged in legitimate political speech critical of the government.

The bill proposes a 24-hour deadline for platforms to remove 'harmful content'. This short timeline means that platforms \*will\* offload responsibility for removing content to unreliable, arbitrary, and (if history is any guide) racist algorithmic models.

When online speech can be removed arbitrarily by non-human pseudo-intelligences for reasons it is impossible for an average citizen to understand, the chilling effect on open discourse in what is now \*the only forum that matters\* will be palpable and kafkaesque.

The provision mandating that platforms report 'potentially harmful' (whatever that could possibly mean) to law enforcement agencies is horrifying.

Law enforcement agencies at \*all levels\* of government have repeatedly shown themselves to untrustworthy arbiters of the public good, and this bill would give them enormous new powers to compile information on, stalk and terrorize both marginalized communities and those who justifiably speak out against their corruption and brutality.

I do not trust law enforcement to use this new power wisely or justly, and I do not think there is any pressing and substantial need to give them this power.

I believe, strongly, that law enforcement has

all the tools and powers it needs to perform it's legitimate function. If they fail to do so, the fault lies in their incompetence and institutional rot: giving them new powers will only enable them to further oppress the innocent.

The bill's proposed data-retention policies are also absurd. They will create huge repositories of data that will never be secure.

I do not trust either the government or technology platforms to keep retained data secure on this scale. I am convinced that leaks of this stored data will inevitably occur, and that when they do this data will be used to stalk, target, advertise to, hack, and blackmail Canadians. I think this part of the proposed policy is irresponsible in the extreme.

Finally, I am horrified that the bill allows each new parliament to shape the contours of this bill, and to appoint an internet czar with broad discretion to expand its worst elements.

Document communique en vertu de la Loi sur l'accès à l'information. Document released pursuant to

To put Canadians' digital freedoms (which now encompass all other freedoms) into the hands of a political appointee is unbelievable folly.

It means the standards and goalposts of what is considered legitimate speech will change from election to election (and how can Canadians have a free and open public discourse if the rules of what is permitted speech can change with the brief lifespan of a minority government?)

It also means that the person responsible for moving those goalposts will invariably be, not a career civil servant or expert, but some amoral political climber chosen for their loyalty to whatever regime currently holds power.

Simply put, I do not trust any appointee

the current government would make to discharge these responsibilities in a manner consistent with the public good, and I trust the other parties to wield this largely arbitrary power \*much less\*.

If nobody can be trusted to wield a power responsibly, I think it should not be created.

In our current political climate, it is also very easy for me to imagine a totalitarian, illiberal, or fascist political party coming to power in Canada's near future. This legislation would be a ready-made tool for such a party to consolidate its gains and destroy political rivals upon its first day in office. I think therefore, that this legislation would have a destructive effect on the resiliency of our democracy.

In conclusion, I think this legislation is too broad, too powerful, and too poorly-thought-out to be brought to the table. I think it should be scrapped.

Furthermore, I think it's a pity that Canada would even consider such legislation when it has some of the finest academic minds in the world working out of places like U of T's Citizen Lab, on ways to preserve a free, sane, and decent internet for all humanity. We have the expertise in this country. We should use it.

Thank you for your consideration,

Alexander Saxton,

s,19(1)

 From:
 Iristan Nuyens

 To:
 ICN / DCI (PCH)

 Subject:
 Approach to addressing harmful content online

 Date:
 August 12, 2021 9:04:48 AM

Hello,

While I agree with the overall idea of this, the approach seems a bit heavy handed and may have some unintended but severe consequences for innocent parties.

Please consider reigning in the power of any 'overseer' of an approach such as this, like the appointment of an Internet Czar by a prime minister.

Thanks, -Tristan Nuyens

Sent from my iPhone

From:	Phil Warder
To:	ICN / DCI (PCH)
Subject:	Harmful Contents Law
Date:	August 12, 2021 8:42:02 AM

This proposed law is scary Orwellian stuff. This can easily be manipulated by the government in power to censor its critics. Very easily. Canada is descending into totalitarianism. The Libreal party is horrible for thinking this is a good idea.

From:	Metal Dragon
To:	ICN / DCI (PCH)
Subject:	Concerning the proposed approach to combatting hateful content online
Date:	August 12, 2021 3:43:57 AM

#### Greetings

It is not only personal belief but also set in stone fact that the proposed strategy to combatting hateful content online will not only be a major overstepping of government control and reach it will also cause incredible amounts of harm to marginalized voices and communities who will be mostly affected by this new set of amendments to bill C-36. The creation of a commission to prosecute and punish harmful content as suggested by what would most likely be an AI based algorithm which have been known to make errors when deciding whether the content it is looking through is offensive or not and has the ability to make unchecked and unprompted investigations into social media platforms would be devastating to freedoms of speech as evidenced by such algorithms in use by youtube having been known to make many mistakes in judging offensive content much to the grief of users of the platform which will also suffer from the overreach and draconian measures implemented by this proposed set of laws.

The punishments levied by the commission would only be able to be paid by large technology companies who have a poor ability to moderate content and attempts to enforce it have only led to widespread user dissatisfaction and miscalls in what was considered "offensive" or judged normally leaving smaller businesses attempting to create their own social media spaces unable to provide a fair and free social space for internet users.

https://twitter.com/doctorow/status/1425469727539798016

https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/

https://twitter.com/daphnehk/status/1421120217585831938

These links also provide apt explanations as to why this new approach would only cause untold amounts of harm to internet users and freedom of expression which this sorely dismisses in favor of draconian and overbearing measures to combat broadly defined harmful content.

Please consider the consequences of implementing these measures- A.M

From:	Lucas Timmons MPE ACCESS to Into
To:	ICN / DCI (PCH)
Subject: Have your say: The Government's proposed approach to address harmful content online	
Date:	August 12, 2021 2:29:06 AM

Hello,

Here are my comments.

This proposed approach is a terrible idea. There is no value to this approach whatsoever. None.

Leaving aside the secretive way the government put this together, the idea itself is counter to democracy.

Here are just a few issues:

People who are already marginalised are disproportionately likely to be censored under rules like this.

Online harms rules are a human rights disaster. They've been roundly criticised by UN Rapporteurs and civil society groups all over the world.

The government should not be in the business of censoring speech, on the internet or elsewhere.

This is a TERRIBLE proposed law and those who thought it up should feel ashamed for doing so.

Do the right thing and abandon this right away.

Lucas Timmons

From:	Maxwell Millar-Blanchaer the Access to Inform	
To:	ICN / DCI (PCH)	
Subject:	Serious concerns about "The Government's proposed approach to address harmful content online"	
Date:	August 12, 2021 1:52:25 AM	

#### Hi there,

I'm writing as a concerned Canadian to express some serious concerns I have about the government's proposed approach to address harmful content online. I'm particularly concerned about a few points:

- the requirement to take down "harmful content" that is legal speech otherwise
- the 24-hour takedown requirement that will result in internet platforms erring on the side of caution and just taking down content without the ability to vet it thoroughly

While I appreciate the end results that the government is after (at least on paper), the strategies suggested here have been tested in other places around the world and have generally resulted in failures in their original goals and have only resulted in the existing tech monopolies gaining more power. The issues are not with specific implementations, but with the overall philosophy. It is my opinion that this effort should be scrapped.

Thank you for your time, Max

From:	Matthew
To:	ICN / DCI (PCH)
Subject:	Re: The Liberal Government's Speech-Throttling legislation
Date:	August 12, 2021 1:29:23 AM

s.19(1)

Hello,

As a Canadian citizen and I am highly alarmed by the proposed legislation to "stitle harmful speech online". As someone who remembers all the lies and secrecy surrounding bill C-10 I am deeply concerned that the Liberal government are catering not to the Canadian people, but to monied interests with a desire to stifle criticism.

A simple, rational consideration of the proposed law leads to the conclusion that there is ZERO reason for tech companies to devote time and resources to actually examining flagged speech and determining whether it is 'lawful'. Instead, with the 24 hour takedown requirement, they will simply block/ban/take down any flagged speech whether it actually falls under the law or not and as likely as not will never bother to review it once the damage is done.

#### https://twitter.com/doctorow/status/1425469727539798016

This thread highlights most of my concerns (barring the personal distrust of the Liberals after being lied to and harmed by their government personally on three separate occasions since helping to get the current PM elected in the first place).

I do not trust the Liberal party to decide what I may or may not post in public fora. I MOST DEFINITELY do not trust the Conservative government that, sooner or later, will ooze back into power and happily use such legislation to silence all criticism and immiserate their critics.

I fail to see how this legislation actually improves things. In fact, I am utterly certain that it will make the lives of marginalized groups (such as myself, as a disabled individual in a wheelchair) worse. It will disrupt and destroy the ability of groups to organize and communicate with one another because any vandal with a grudge will be able to flag speech spuriously and have it removed within a day.

The lack of any penalty for flagging speech falsely is the greatest problem I have with this disastrous piece of cryptofascist drek, but it is scarcely the only one. I ask you please to reconsider this.

This does not protect anyone but those who specifically want to silence all criticism. This does not preserve MY CHARTER RIGHTS. This is bad law.

Stop it.

Sincerely,

A dissatisfied, disgruntled and malcontented Canadian Voter.

From:	cris fraenkel
To:	ICN / DCI (PCH)
Date:	August 12, 2021 12:55:55 AM

I am commenting on the governments plan to empower internet providers to become the next supercharged police force online.

Specifically, your request for comments here: <u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html</u>

You are taking a well intentioned attempt at solving a relatively small, relatively isolated problem, but using an approach that will cause our whole society much more harm than the problem you're trying to fix.

## Specifically

- your arbitrary 24 hour deadline for taking action ensures no chance of considered, human review. Reacting that fast to the huge quantity of new content can only be done by automatic filters. Every time this has been attempted, it has failed miserably.... examples include being unable critique issues because you can't talk about them without getting banned, and completely off-topic content being banned because they happened to use too many triggering words (in a different context - but algorithms can't know that)

- huge penalties for failure to remove deemed 'harmful' speech, but no penalties for removing permitted speech in error guarantees a 'shoot now, ask questions later' approach, with 'later' meaning 'never'.

- the technical difficulty and cost of meeting your requirements are a gift to Facebook, Twitter, Apple and the like. No new competitors could ever hope to compete, cementing their stranglehold on online discussion.

Do not make the problem worse (which this will do).

sincerely

Cris Fraenkel

s.19(1)

 From:
 Alex Elrick

 To:
 ICN / DCI (PCH)

 Subject:
 Issues regarding bill on "Harmful Content Online"

 Date:
 August 11, 2021 11:39:54 PM

-Permitting algorithmic detection will likely allow offenders to continue while innocents are punished, see also algorithmic detection of copyright infringement

-Requiring robust systems of detection will require companies have sizable budgets for such, pushing out smaller players (contributing to monopolization)

-Same as above, but regarding data retention.

-24 hour response times leave too little room for review

-Too much leeway is given to companies regarding enforcement and decisions on what content is harmful; they shouldn't have the power. Content from marginalized individuals is more commonly censored

-No penalty for (intentionally or unintentionally) blocking acceptable content will have companies erring on the side of censorship

 From:
 Bigg
 Merce

 To:
 ICN / DCI (PCH)

 Subject:
 The Government's proposed approach to address harmful content online

 Date:
 August 11, 2021 11:16:22 PM

I'm a Canadian citizen writing in to protest proposed changes to Canadian legislation (detailed here) which will introduce a swath of horrendous, untenable legal obligations for social media platforms to remove vaguely-defined "lawful-but-awful" speech. I emphatically oppose these legislative changes, which will chill free expression by Canadians in the worst ways, and most severely impact already-marginalized groups. I also protest the rushed and secretive means by which these legislative changes are being hurried forward, without proper consultation or even notification for constituents. I strongly urge the government to abandon this atrocious legislation and undergo a proper, thorough consultation process that is honest and just for the millions of Canadians who use the internet.

- Malcolm Christiansen s.19(1)

Sent with Secure Email.

From:	Cameron Bethell MDE ADDE
To:	ICN / DCI (PCH)
Subject:	RE: The Government's proposed approach to address harmful content online
Date:	August 11, 2021 11:00:47 PM

To whom it may concern,

s.19(1)

There is too much grey area in interpreting harmful content and enforcing "justice" in this approach. It is simply a step in the wrong direction. We should improve our education system on these topics and increase funding to social systems that uplift and empower Canadians to create and foster the media we each want to see and take part in.

now and I've been quite actively online since I was a teenager. Even twenty years ago I understood and would avoid the content that is being discussed for regulation with this proposal. It's extremely important to our engagement with online content that Canadians feel empowered by our laws, not in fear of a system that will inevitably be abused and implemented unjustly.

Thank you, Cameron Bethell

From:	Alexander Hoffer
To:	ICN / DCI (PCH)
Subject:	Comment on The Government's proposed approach to address "harmful content" online
Date:	August 11, 2021 10:48:15 PM

Hello,

I recently came across the Trudeau government proposal for regulatory for 'harmful' content online: <u>https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html</u>. This is all despite the lack of publicity or any kind of requests for comments.

My comment regarding this is brief: This is an absolutely atrocious and horrendous proposal, will not actually solve the problems aimed at it, and will instead create more costs and burdens on average Canadians and decreasing our freedoms while increasing their costs to implement a lot of the proposed policies. I can not believe that this is even being considered, as this is an amalgation of all of the worst policies that have been done and tried throughout the world. France for example had something like this that was nowhere near as extreme as proposed here and it was ruled as unconstitutional:

https://www.eff.org/press/releases/victory-french-high-court-rules-most-hate-speech-bill-would-undermine-freeexpression

This is the kind of stuff I expect out of totalitarian dictator ships like China and Russia, especially with the idea of any harmful content that a provider won't take down (what are you going to do about entities outside of Canada that you have no influence over?) that is to make a national Chinese like firewall. I also happen to work at an independent telecommunications company, and just the idea of having to implement this while passing on the costs to our customers is just terrible. If the prices are not passed on by an ISP, this will be an additional cost we will have to pay for in our federal taxes, which is terrible.

My suggestion is that you scrap this entirely (along with Bill C-10), and actually look at ways of improving Canadian's privacy, and fighting the various monopolies (including the giant Canadian telcos, not coddling them and thinking you can protect us from them), and other more valuable things like right to repair, etc. This regulatory framework is entirely the wrong approach to be doing, and a far better use of our tax payer dollars. This regulatory proposal will not solve the problems it aims to and will just create more problems and decrease our freedom as a democratic society. Proposals like these is why I don't vote for the Liberal government, since this seems like something a Conservative government would propose as well, whom I also do not vote for usually.

Thank you for reading, and please consider my points above to roll back this proposal.

- Alexander Hoffer s.

s.19(1)

From:	Harry Glynn
To:	ICN / DCI (PCH)
Subject:	Harmful content bill
Date:	August 11, 2021 10:17:39 PM

Hello,

As a Canadian I am strongly against this bill. While well intentioned, I simply do not trust corporations to get moderation perfect. The bill requires far too fast an adjudication process and harsh punishments for non-compliance. This means that regular speech is likely to be censored and caught up in the dragnet of this policy's implementation.

While I deplore hate speech and misinformation, curbing it can't come at the cost of our liberties and free speech. In Canada we are a free country first and foremost. If regulation intended to achieve some good sacrifices such a core tenet of our country's values it cannot be allowed to pass.

Good day

Harry

 From:
 Aaron V. Humphrey

 To:
 ICN / DCI (PCH)

 Subject:
 Censoring Online Harmful Content Considered Harmful

 Date:
 August 11, 2021 10:17:13 PM

This proposal is an awful, awful idea. It is implemented in a ridiculous fashion, worse than France's unconstitutional version, and it will only continue to entrench social media monopolies that we should instead be trying to whittle down. Any policy which can only be done by a large company will do more harm than good, and automated tools are nowhere near good enough for this. The lack of penalties for false positives will mean that excessive content will be removed due to "better safe than sorry" policies.

Online hate groups are bad, sure, but this will do more harm than good. Who gets to decide what speech is "harmful"? All it takes is for the government internet czar to decide that "Antifa", "Black Lives Matter", and "Defund The Police" are hate speech (as bad-faith actors keep trying to paint them as), and this will have the opposite of its purportedly intended purpose.

I'm sure plenty of other organizations have better ideas as to how this could be done without turning this into an Orwellian nightmare, and I don't mean big social media companies here.

Don't do this.

From:	Devon Wiersma
To:	ICN / DCI (PCH)
Subject:	Feedback on Proposed "Harmful Online Content" Strategy
Date:	August 11, 2021 10:12:08 PM

#### Hello,

I'm writing to have my voice heard with regards to the Government's Approach to implement a broad, vague and dangerous internet-censorship strategy which will ultimately cause harm to marginalized individuals.

While child abuse and exploitation is a very real issue, many of the reforms proposed within the guideline to combat this put ownership on large tech companies to comply with these issues in a rushed manner, which is going to have unintended side-effects of causing them to air on the side of caution and implement crackdowns on all forms of content, including but not exclusive to, those of marginalized individuals such as black and trans people. There are many documented cases of similar effect occurring in other countries who have implemented similar laws that, while well-intended, result in the systemic endangerment of many marginalized individuals due to guidelines which are both too wide-reaching and broad to be targeted effectively and in a measured manner.

For more information as to why the proposed guidelines are reckless and serve to endanger marginalized populations due to excessive requirements, please take a look at <u>this well-written</u> <u>article by the EFF</u> breaking down some of the issues these requirements would cause.

I am wary that these proposed guidelines are a step in the wrong direction that will simply enable the suppression and destruction of marginalized identities even further simply because the government fast-tracked a plan without fully considering the implications of how that plan could effectively be acted on by the corporations it is targetting, and the fallout from their responses which would effectively do more further damage.

 From:
 Daniel James

 To:
 ICN / DCI (PCH)

 Subject:
 Comments on Harmful Online Content proposal

 Date:
 August 11, 2021 10:04:37 PM

To whom it may concern,

I wish to register my objection to these proposals. I am a Canadian citizen, internet entrepreneur since 1994 and former manager at Facebook. My family and I live in California for economic reasons. A few key points from my perspective:

- Implementation of a 'Chinese wall' style filtering system for the Canadian internet will help to encourage migration to the US and other countries.

- Onerous requirements for complex, automated filtering systems and expensive, fast turnaround human support will have a chilling effect on the development of competitive social systems to the tech giant monopolies.

- These measures will not improve public safety. Dangerous people (along with everyone else) use private, encrypted messaging that is not covered by this bill (nor should be legislated against for numerous reasons, not least impracticability). Instead, vast numbers of false positives will leave an immortal store of personal information in the hands of multiple agencies.

- It's very clear that everyone who understands cyber law thinks this is a terrible idea. For example, with more legal details: <u>https://twitter.com/daphnehk/status/1421118036895961094</u>

thanks for your consideration, please please scrap this rubbish,

- Daniel

Thank you

- Daniel

From:	rian currie
To:	ICN / DCI (PCH)
Subject:	Bill C-36 response
Date:	August 11, 2021 10:01:39 PM

### Hello,

Bill C-36 directly violates the canadian charter of rights and freedoms, specifically section 2b: "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication", in that it requires companies to remove "harmful content" which includes speech that is legal but potentially upsetting or harmful. This includes speech criticising the government and public figures for their actions.

Bill C-36 also includes mandatory reporting of "potentially harmful content" as well as the users who post such content to law enforcement and national security agencies. This also violates section 2b of the charter of rights and freedoms as what is deemed "potentially harmful content" is decided in secret by the government and again may include criticism of the government and public figures.

In short, I oppose Bill C-36 as it would create a chilling effect within Canada when it comes to freedom of speech and expression.

 From:
 Richard Yates

 To:
 ICN / DCI (PCH)

 Subject:
 censorship & "the new" regulations and law

 Date:
 August 11, 2021 9:24:17 PM

There is already a deadening censorship going on. And your proposed "regulations" and new law would only go toward abetting the increasing censorship of minority views.

Here is a specific case of a Canadian journalist who has been gagged and removed by the social media companies and their brain-dead "algorithms:

https://taibbi.substack.com/p/meet-the-censored-paul-jay

Your proposed regulations & law would only worsen what is becoming a dangerous and deteriorating situation. You claim to be trying to "protect" Canadians, but the bigger problem is that already you have lost control of the Internet to big US tech companies and their brain-dead algorithms.

What you propose will only make a bad situation worse.

And I find it disgusting that you are proposing these new regulations and law without any real attempt to "seek consultation" with the Canadian public. And it is clear that you are doing this without any input from well-known critics of Internet policy like Michael Geist, the Canada Research Chair in Internet and E-Commerce Law at the University of Ottawa and a member of the Centre for Law, Technology and Society.

It is absolutely DISGUSTING that you would make this manoeuvre without consulting an expert like Michael Geist.

Your "regulations" and new law are a sham. And worse than that. They will backfire and blow up and make a bad situation worse... and you are TOO STUPID to realize it!!!

I am:

s.19(1)

 From:
 Joé McKen

 To:
 ICN / DCI (PCH)

 Subject:
 Proposed "harmful content" legislation

 Date:
 August 11, 2021 9:17:08 PM

### Hello,

I'm writing to express my deep concerns regarding the Liberal government's proposed regulatory framework for taking down harmful Internet content. As a Canadian citizen, I enjoy living in a country with a free and open Internet. I fear this proposed legislation will cause serious harm to every Canadian's online experience – including and especially people who were never intended to be targeted by the law.

The sad but simple truth is that it is impossible to craft legislation that will solely target the intended wrongdoing of a few. Every time such "anti-harmful content" legislation has been tried, both domestically and internationally, it has been by all reasonable measures a failure, with platforms being compelled to remove perfectly lawful and legitimate speech. Multiple countries across the world, notably around Europe, have implemented such laws in recent years, and every one of them, without exception, has chilled their populace's expression, eroding one of a free society's most important freedoms. Some of those countries were even forced to scrap those laws not long after implementation, such as in France, where a similar law regulating Internet content was abolished by the courts.

Worse, this Canadian initiative appears to include all the most troubling and dangerous elements of its contemporaries in one package. It targets speech that is merely upsetting or immoral but not actually illegal, effectively violating the country's free speech laws in spirit if not in letter; it imposes a 24-hour window for companies to comply with takedown requests, which is *far* too short to allow any consideration of context or nuance, guaranteeing that a vast amount of legal content will be removed; its data-retention policy will force Internet companies to spy on their users; it adds website-blocking regime that will censor any space deemed a repeat offender by the government with little apparent oversight; and it includes stiff penalties for service providers who fail to remove flagged content fast enough for the government's liking, which all but ensures the strictest and most heavy-handed enforcement. The only way companies can effectively comply with these onerous new rules would be by implementing strict automated upload filters that will necessarily prevent the publication of a vast amount of legitimate content and discussion.

Any of these measures on their own would run counter to the spirit of a free and open Internet; combining them into a single regulatory package guarantees disaster. Canada would effectively have the most restrictive and least free Internet of any modern democracy. It would be a national shame, at least until public outcry – which, once people realize just how limited their Internet will have become under this law, is certain to be swift, vociferous, and lasting – inevitably forces the law's repeal.

These harms aren't hypothetical; for an example of how dangerous these "protecting victims" laws can be, we need only look south of the border. A few years ago the United States federal government proposed, debated and ultimately passed a package of legislation known as FOSTA-SESTA that promised to help combat online sex trafficking. Free-speech experts and civil-liberties advocates, as well as anti-sex-trafficking activists, warned from the beginning that the law would unavoidably result in suppressing legitimate speech, endanger consensual

# Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

sex workers, and likely fail to meaningfully help sex-trafficking victims, but they were signored. When the law was passed, the results were swift and unambiguous: Numerous websites restricted or outright prohibited any adult content in fear of running afoul of the new law, with some platforms shutting down altogether; sex workers were forced out of spaces where they had previously organized and shared safety information, putting them at greater risk of harm; and as for sex trafficking, multiple studies and advocacy groups concluded the law had little to no meaningful impact on its prevalence, and if anything made law enforcement's job of finding traffickers and victims more difficult by removing them from public view. Effectively, the law not only caused significant collateral damage, it likely worsened the very problem it was meant to address – exactly as subject-matter experts had warned would happen.

Now, it may be easy to read the above and think that surely what happened in different countries doesn't inform us of what may happen in this country, or to conclude that those unintended consequences can be averted by simply writing this law better, tweaking this bit and clarifying that clause and so on. But history has shown there is a remarkable consistency in how the Internet operates across borders, and in how laws enacted in different nations play out. It would be a grave mistake to look at the track record of these anti-harmful-content laws failing in their goals and wreaking havoc upon the rights of citizenries around the world and to assume that the same will not happen here. The pattern is clear, and we ignore it at our peril.

No civilized person will defend the kinds of content this law is intended to address. Their harms are concrete and devastating. But as an ardent supporter of civil liberties, I strongly believe that the right solution to any problem is not one that is likely to create new and bigger problems for others, curtailing basic freedoms and putting innocents in legal jeopardy. We cannot answering violations of rights with more violations of other rights. In addition to raising issues of basic fairness and justice, it flies in the face of the professed ideals and essential liberty that are enshrined in the heart of any true democracy.

I don't pretend to know what the answer to harmful content is. But I do know, beyond any doubt, that this legislation isn't it. Some of the very smartest and most experienced policy experts and technologists, both in Canada and around the world, are warning you about the dangers of this law. I beg you to heed them.

Sincerely yours, – Joé McKen

Twitter | Bandcamp | YouTube | SoundCloud

 From:
 Klaus Steden

 To:
 ICN / DCI (PCH)

 Subject:
 Proposed approach to address harmful content online

 Date:
 August 11, 2021 7:49:41 PM

To whom it may concern,

I am writing today to provide feedback about changes the federal government is proposing in Bill C-36 with respect to a new regulatory framework for social media platforms.

The proposed framework is comprehensively terrible. It invests far too much authority in the moderation algorithms and personnel at large social media platforms who have already demonstrated themselves to be poor custodians of free speech.

It makes it far too easy for large platforms to silence or marginalize voices from already marginalized communities: sex workers, anti-racists, indigenous activists, police reformers, etc., communities that have already been subjected to measurable harms by previous approaches to moderation, even well-intentioned ones that were ultimately badly flawed.

It does nothing to address the massive antitrust problems of existing social media giants and gives wealthy players in the space significant advantages due to their scale and financial resources, effectively shutting out any meaningful competition from upstarts.

It invests too much authority in the hands of a single individual, namely, the Orwelliansounding Digital Safety Commissioner. This office is ripe for misuse by the federal government, and four years of President Trump in the United States has brought into extremely sharp focus that concerns like this are not abstract. Canada does not have a monopoly on virtuous government, so baking risks like this directly into the body politic is simply reckless.

Finally, the reporting and enforcement framework is deeply troubling. Requiring ISPs to act as gatekeepers is no less problematic than entrusting this responsibility to social media platforms. The enforcement window is ludicrously short, and will invariably result in a "shoot first, ask questions later maybe if at all" approach to content regulation that, again, is likely to be overwhelmingly biased against already marginalized communities. Placing the ISPs in a position to dictate what is and isn't acceptable to Canadians puts Canada on a dangerous path towards a "Great Firewall of China" model, but one that is arguably even worse, because I can't vote Bell or Rogers out of office if one of them acts counter to the public interest. It is no secret how easy it is to weaponize power like this, and a framework that is so reliant on the goodwill of both bureaucrats and industry is unworkable.

We have seen already this year with the C-10 fracas that this federal government is more than willing to sell off our interests as voters to big business when it suits their purpose, and that the government's commitment to online free speech shifts with the political wind. That is no solution at all, and as Canadians, we deserve better.

sincerely, Klaus Steden s.19(1)

s.19(1)

 From:
 Keith Mann

 To:
 ICN / DCI (PCH)

 Subject:
 Comments re: proposed harmful online content regulation

 Date:
 August 11, 2021 7:41:45 PM

I am writing to express my deep concern about the shortcomings of the government's proposed legislation to address harmful content online.

https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/) and Cory Doctorow ( https://pluralistic.net/2021/08/11/the-canada-variant/#no-canada and https://www.eff.org/deeplinks/2021/08/utilities-governed-empires) and supported by research such as this: https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filtering-

https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filteringblocking-and-reporting-rules-1

I urge the government to consider these shortcomings and amend the proposal so as to thoroughly address them. They pose a serious risk to the rights and the safety of Canadians.

Sincerely,

Keith J. Mann

s.19(1)

From:	Thomas Fillingham
To:	ICN / DCI (PCH)
Subject:	feedback
Date:	August 11, 2021 7:24:05 PM

The July 29 2021 release of a proposed framework for an Act of Parliament to regulate Online Communication Services is a grave danger to the charter of rights and freedoms that we as Canadians have adopted as our rights in our supposed free and democratic country. I object with every ounce of my being the poorly thought out and authoritarian measures being proposed by this act and call for a rejection of all these proposals and a new commission be established to study the matter in a more rigorous way to ensure that the rights of Canadians will not be ignored by such legislation.

DO YOU UNDERSTAND WHAT I AM SAYING HERE? I AM COMPLETELY OPPOSED TO WHAT YOU ARE PROPOSING, IS IS EXTREMELY POORLY THOUGHT OUT AT BEST, AND VERGING ON TOTAL INCOMPETENCE OR DELIBERATE AUTHORITARIANISM AT WORST. UNLESS YOU AS A GOVERNMENT ARE DELIBERATELY TRYING TO ASSUME POWERS THAT DO NOT BELONG TO YOU I DEMAND THAT YOU CEASE THIS SHAMEFUL ACTIVITY IMMEDIATELY OR I WILL DO EVERYTHING IN MY POWER TO REMOVE YOU FROM OFFICE COME THE NEXT ELECTION. GIVE THIS ATTEMPT AT NEEDED LEGISLATION THE PROPER DELIBERATION IT NEEDS BEFORE YOU SHAMELESSLY STRIP US OF OUR RIGHTS!

SHAME ON YOU PIERRE TRUDEAU AND YOU SUPPOSED LIBERALS!

From:	Caitlin Lucy Henderson
To:	ICN / DCI (PCH)
Subject:	Proposed approach to address harmful content online is seriously flawed.
Date:	August 11, 2021 7:06:02 PM

Hello,

I'm writing to express my disappointment with the proposed approach to address harmful content online and to state my complete opposition to this regulation in its current state. While harmful online content is a real problem, the proposed regulation is not a real solution. It is too broad to be useful, while draconian enough to be dangerous.

The 24-hour deadline for removal of undefined 'harmful content' guarantees that platforms will not have time to conduct a thorough analysis of speech before it is censored. It also creates a de-facto requirement for platforms to install algorithmic filters to (mis)identify and remove prohibited expression, as it would otherwise be impossible to meet the 24-hour deadline. Yet these algorithmic filters have a proven track record of inaccuracy and bias, especially against marginalized people.

The proposal's combination of prohibiting poorly defined 'harmful content', harsh penalties for not blocking with no penalties for wrongfully blocking, and requiring swift compliance without time for adequate assessment means that this regulation will almost certainly be struck down as unconstitutional, as were similar regulations in France and other countries.

The USA's version of this regulation, SESTA-FOSTA, was unable to prevent or even slow down the spread of Covid-19 misinformation or the Q-Anon conspiracy, proving that this approach to addressing harmful content online does not work. Better strategies include breaking up big tech monopolies and limiting how much information they are allowed to collect on their users

Please scrap the proposed regulation and start again from the beginning,

Caitlin Henderson

From:	Jalgris Hodson ME ACCESS TO
To:	ICN / DCI (PCH)
Subject:	feedback on the Government"s proposed approach to address harmful content online
Date:	August 11, 2021 6:48:00 PM

#### Hello,

My name is Jaigris Hodson, and I'm an Associate Professor at Royal Roads University where I am also the Canada Research Chair in digital communication for the public interest. My research is concerned with understanding harmful online content, including online abuse, conspiracy theories and medical information, and I am writing to you as an expert in the field to say that I do not support the proposed legislation and think it is misguided and potentially harmful to the best interests of the Canadian public.

Th UN Rapporteurs and other cilvil society groups around the world have already critiqued online harms rules like the ones being proposed in this legislation. Frankly, they're the wrong tools for the job, and they will cause smaller minority online voices to suffer, while protecting the large platforms that most benefit from current online harmful speech. This proposed law will ensure that large tech giants like Facebook remain arbiters of speech, because imposing a duty to spend millions of dollars on speech filters is something only the largest tech companies can afford. This flies in the face of what we should be doing, which is finding ways to limit the power and influence of tech giants in this Country. We should be supporting rules that support smaller technology companies, not ones that make it impossible for smaller tech competitors to thrive.

These laws present a host of negative consequences, many of which are probably unintended. I do not support it, and I believe it is not in the best interests of thriving democratic communication in Canada. Thank you,

Jaigris

Jalgris Hodson Php, Associate Professor, College of Interdisciplinary Studies | Royal Roads University T 250.391.2600 | F 250.391.2587 2005 Sooke Road, Victoria, BC Canada V9B 5Y2 | royalroads.ca Pronouns: she/her/hers

#### LIFE.CHANGING

Royal Roads is located on the traditional lands of the Xwsepsum and Lekwungen First Nations' ancestors and families.

CONFIDENTIALITY NOTICE: This e-mail and attachments may contain personal or confidential information for the sole use of the intended recipient. If you are not the intended recipient and you have received this transmission in error, please notify the sender immediately and delete the message and attachments.

Royal Roads is located on the traditional lands of the Xwsepsum and Lekwungen ancestors and families.

CONFIDENTIALITY NOTICE: This e-mail and attachments may contain personal or confidential information for the sole use of the intended recipient. If you are not the intended recipient and you have received this transmission in error, please notify the sender immediately and delete the message and attachments.

Dear government

NO NO and HELL NO

to just about every marxist dystopian coup d'etat move you make. LEAVE FREE SPEECH ALONE

LEAVE FREE INTENET FREE SPEECH ALONE AND STAND DOWN AS YOU HAVE LOST ALL RIGHT TO GOVERN AND I HAVE LOST ALL FAITH IN THIS DEMONIC SATANIC UNSCIENTIFIC LYING GROUP OF BOUGHT AND PAID FOR USEFUL IDIOTS

THERE IS NO ISOLATED VIRUS SPECIMEN ANYWHERE IN THE WORLD NO COVID ONLY A MASSIVE LONG PLANNED AND PATENTED FRAUD AND THE GREATEST CRIME EVER COMITTED AGAINST HUMANITY.

STOP WITH THE KHALERGI PLAN STOP WITH THE NEW WORLD ORDER ONE WORLD GOVT COUP D'ETAT STOP WITH THE GENOCIDE AND THE INJECTIONS THAT HAVE KILLED AN ESTIMATED 2 MILLION NOW AND MAIMED OH SO MANY MORE.

VAERS DATA ENDURAVIGILANCE DATA UK YELLOW CARD SCHEME DATA

5 year all cause mortality tells the story too!!

WE ARE NOT STUPIDIIIIIIII YOU ARE ALL CRIMINALS NOW AND WILL BE CHARGED FOR CRIMES AGAINST HUMANITY SOON ENOUGH.

and WE WILL NOT BE JOINING YOUR BEAST SYSTEM EITHER.

Cal Aylmer



Cânadian. lewish. Advocacy

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Acl.

Submission for the Government of Canada's Proposed Approach to Combat Online Harms

September 15th, 2021

Thank you for the opportunity to submit comments regarding the Government of Canada's proposed online harms legislation.

The Centre for Israel and Jewish Affairs (CIJA) is the advocacy agent of the Jewish Federations of Canada. We are a non-profit, non-partisan organization dedicated to preserving and protecting Jewish life in Canada through advocacy. CIJA represents more than 150,000 Jewish Canadians from coast to coast, via the Federation system.

CIJA has long advocated against antisemitism, hate, and terrorism. While the government's consultation is expansive – including five areas of deplorable online harms — our submission is limited to CIJA's areas of expertise: online hate and terrorism.

The rise of online hate is a serious concern for Jewish Canadians, as is the protection of freedom of expression — a cornerstone of Canadian democracy. It is, therefore, imperative that the online harms legislation strike the correct balance between freedom of expression and protection against online hate.

The threat of online hate is real. A recent report from the Center for Countering Digital Hatred (CCDH) found that, on average, 84 per cent of reported antisemitic social media posts on Facebook, Twitter, TikTok, Instagram, and YouTube did not engender responses from the platforms. Alarmingly, the 700 social media posts studied in the CCDH report were collectively viewed 7.3 million times<sup>1</sup>; a total greater than the population of Toronto, Montreal, Calgary, and Ottawa combined<sup>2</sup>. Online antisemitism takes many forms, including Holocaust denial, promotion of classic or historic stereotypes, antisemitic tropes, and promotion of contemporary Jew-hatred. Jewish Canadians know first-hand that online harm has real world consequences: bullying, exclusion and discrimination of individuals, and attacks on community and religious institutions.

CIJA welcomes many aspects of the government's proposal:

- An independent regulatory regime. We have long called for a regulatory structure that includes an independent regulator, and we are pleased that the proposed consultation includes the establishment of the independent Digital Safety Commissioner and a regulatory framework. An independent regulator provides an important function to combat online hate. Some content may be unpopular, hurtful, or detestable. An independent regulator ensures that the decisions made are impartial. The independence of the digital safety advocate is, therefore, critical to making decisions on messages that, although unpopular, are nevertheless a component of freedom of expression in a liberal democracy.
- Definition of hate aligning with Supreme Court of Canada jurisprudence. This provides a reliable and consistent measure through which to define online hate. Doing so sets the standard to ensure that the proposed legislation will address hate, while protecting freedom of expression.
- Annual reports. We are pleased that that the Government's proposal will mandate annual progress reports. Transparency and accountability are important hallmarks to combat online hate.

<sup>&</sup>lt;sup>1</sup> Anti-Semitic social posts 'not taken down' in 80% of cases - BBC News

<sup>&</sup>lt;sup>2</sup> https://www12.statcan.gc.ca/census-recensement/2016/as-sa/98-200-x/2016001/98-200-x2016001-eng.cfm

- Penalties for non-compliance. Effective legislation needs effective enforcement. Thus, we also welcome
  the Government of Canada's proposed monetary penalties for social media companies for noncompliance.
- The complaint process. CIJA has consistently called for a process that puts the onus on social media companies as the 'first stop' to deal with online harms on their respective platforms. The Government of Canada's process mandates social media companies respond in a timely fashion to user complaints and provide a clear appeal process, after which a user can further appeal to the Digital Safety Commission. We agree that the initial process to address online harms should be administered by the respective social media platforms, and we applaud this aspect of the Government's proposal.

While we welcome the Government's proposal, we respectfully submit the following recommendations for your consideration:

- Compelling social media to be frontline first responders. Ensuring that legislation and regulations compel social media companies to address online harms through an obligation of result, as opposed to an obligation of best effort. Whether this is compelling algorithms to pre-emptively take down online hate, or employing the resources to adjudicate complaints, we believe that, when it comes to combating online harms, efforts are not in and of themselves sufficient benchmarks. Instead, outcomes must be used to measure social media company compliance. We recommend that ensuring all legislation and regulations compel social media companies through an obligation of result will put the focus on effective program implementation.
- Connecting legislation to Canada's anti-racism strategy. While we are pleased to see the proposal align with the Supreme Court of Canada's definition of hate, we believe that effective program implementation must also have substantial linkages to *Building a Foundation for Change*, Canada's anti-racism strategy, by including the important definitions of hate contained in the strategy. For Jewish Canadians, this is pertinent because Canada's anti-racism strategy includes the International Holocaust Remembrance Alliance (IHRA) working definition of antisemitism. The IHRA definition is the world's foremost recognized and accepted definition provides context-specific guidance to identify and combat instances of antisemitism.
- Strengthening enforcement tools. While we welcome the penalties against social media companies for non-compliance, we believe that more is needed to enforce the legislative requirements. Rendering social media executives and Board members personally liable would increase accountability and compliance.
- Public education campaigns. While regulatory enforcement is important and necessary, it should be enhanced by general education. We recommend that the online harms legislation compel social media companies to run digital citizenry campaigns at regular intervals. Education is critical to combating hate, especially when we consider that many users of social media are young. For example, a 2020 research paper, *Spreading Hate on TikTok*, prepared by professors from the Institute for Counter Terrorism in Herzliya, Israel, says that TikTok is the fastest growing social media app in the world and has garnered a large youth following with 41% of users between the ages of 16 and 24 years old, with 90% of TikTok users saying they view the app daily<sup>3</sup>. There are also other reports that indicate that many users are under 16 years old<sup>4</sup>. General education campaigns are critical, even more so given the high usage of social media by Canada's youth. One educational approach is for the Government to model public campaigns similar to the legalization of cannabis and defined in *the Cannabis Act*, which includes raising awareness, preventing problematic use, promoting healthy choices, and protecting youth.

<sup>&</sup>lt;sup>3</sup> Weimann, Gabriel and Masri, Natalie. "Research Note: Spreading Hate on TikTok." *Studies in Conflict and Terrorism*. (2020): https://doi.org/10.1080/1057610X.2020.1780027 <sup>4</sup> https://www.statista.com/statistics/1095196/tiktok-us-age-gender-reach/

3 | Page

# Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act.

Finally, we would like to address the **obligation of social media companies to report hate to law enforcement**. The Online Harms Discussion Guide offers two options. One requires regulated entities to notify law enforcement when there is an "imminent risk of serious harm" to a person or property as from online content. The second requires regulated entities to report specific types of "potentially criminal content" directly to law enforcement.

Keeping in mind the goal of balancing civil liberties and protection from online harm, we believe that neither of these options is sufficient to address the unique and varied manifestations of harm presented in the consultation. A one-size-fits-all model is not appropriate. While online hate may be detestable, it may not be comparable to the imminent risk or serious harm caused by a potentially pending terrorist attack. Put simply, with respect to reporting to police, the threat of bombing a building is not the same as espousing hatred.

We offer a third option. We propose the Government adopt a two-track method that requires imminent and serious threats to be reported to *appropriate* law enforcement (such as CSIS, RCMP and RCMP), while other hateful posts be reviewed to determine if they merit being referred to *local police*. We also suggest that the Government establish clear statutory limits on which particular law enforcement agencies are involved in situations of general online hate with a goal of limiting the referral only to necessary agencies.

Thank you for your efforts to tackle online hate and terrorism through the online harms consultation. We are grateful for the opportunity to submit comments and constructively contribute to a safer Canada.

We look forward to working with you on policy proposals that will benefit all Canadians. We are happy to answer any question you may have and are available at <a href="mailto:sfogel@cija.ca">sfogel@cija.ca</a>.

Kindest regards,

Shimon Koffler Fogel President & Chief Executive Officer

From:	Abdihakim Wehelie
To:	ICN / DCI (PCH)
Subject:	Overturn the bill
Date:	August 11, 2021 5:51:54 PM

Hello. While the new Internet regulations are meant to make the Internet safe by imposing restrictions and filters on websites, all it will do is make communication on sites that aren't Facebook/Twitter exceeding difficult because any other site cannot afford the filters imposed, further growing platforms that have too much power over the web with no oversight while killing any hope of alternative spaces. Not to mention that trusting filters to regulate hate speech and sex trafficking is irresponsible in general since there are spaces that marginalized people discuss things like sex work and how to keep each other safe that filters will lump in with sex trafficking or share content that isn't harmful, but will get hit by censors because doesn't fit the vision of who's responsible for restrictions. Please overturn this as this is an infringement of freedom of people and will so much more harm to people (especially marginalized communities) than good.

- Abdihakim Wehelie

From:	Tim Gensey the Access to Information	Ĭ.
To:	ICN / DCI (PCH)	
Subject:	Concerns with the Government of Canada"s plans to deal with Hate Speech, Sex Trafficking, Terrorist content, and other harmful internet content	
Date:	August 11, 2021 4:45:24 PM	

To whomever this may concern

The proposed framwork working through parliment to deal with Hate Speech, Sex Trafficking, Terrorist Content, and other harmful internet content (further referred to as harmul content) is misguided. It will likely fail in stopping malicious actors from harming Canadians domestically and abroad while punishing Canadians for legal participation in their democracy.

Primarily, the effects on all speech are negative. According to Statisa, in 2019 77% of surveyed Canadians rely on the internet as a source of news and about half of them use social media. ISPs under the proposed framework would be subject to opaque guidence, 24 hour compliance time lines, strict fines, and police raids for non compliance. On the other hand, no remedy exists for ISPs or Canadians who are incorrectly targeted. This sets incentives for aggressive and non-responsive removal of legal speech. Given that many Canadians rely on the internet for news and expression, this is equivalent to the Government empowering chosen private deputies to crush printing presses of those spreading content the government does or does not label harmful. A fundamental violation of our most fundamental right of speech.

Despite the massive cost, these systems are easily circumvented. Commercial VPNs and tools for dissidents easily circumvent ISP filters and other proposed tools to combat harmful content. In the US, similar legislation aimed at protectinf women from sex trafficking has not stopped traffickers, but has made life for legal sex workers by removing their ability to advocate and defend themselves. All the while sex traffickers continue to use underground methods to harm women. A similar fate awaits Canadian sex workers and marginalized people if the Federal government pushes forward with such a framework.

The proposed framework strips Canadians of a basic freedom while providing no additional security to vulnerable Canadians. The desire to protect such Canadians is admirable. The proposed framework does no such thing and must be reconsiderred. As a humble civil servant, I implore you to drop this framework and start again based on open discourse with all people living in Canada.

Thank You Tim Gensey CMHC-SCHL

 From:
 Patrick Walsh
 INE\_ACCESS to In

 To:
 ICN / DCI (PCH)

 Subject:
 Have your say: The Government's proposed approach to address harmful content online

 Date:
 August 11, 2021 4:32:56 PM

Thank you for asking for the public to comment on this.

I am happy for all my comments to go on record, and am happy to come testify in person.

The plans to regulate social media and the internet, are wrong, stupid, technically impossible and should be stopped as soon as possible.

Who asked for this?

This sort of attack on freedom should be voted on.

Patrick Walsh

s.19(1)

Evan Sutter ME ADD
ICN / DCI (PCH)
In opposition to the proposed approach to address harmful content online
August 11, 2021 3:32:55 PM

Let me begin by saying that I do believe in the need to curtail the free distribution of hate speech, however this proposition is a dangerous way to try to solve the problem. Frankly, it needs to be *dismissed entirely*. Let me explain.

The proposed solution has several substantial faults that cannot be reconciled within its framing.

- The content moderation that's demanded is unsustainable. The harsh penalties and tight deadlines imposed on OCSs will effectively enforce a "shoot first and ask questions later" policy within these companies. In order to avoid punishment, companies will need to be aggressive in filtering out content. Let me tell you, anyone that pays attention to this space knows that the moderation of these companies is extremely poor and frequently results in false positives. This will undoubtedly damage the free and legal expression of Candians online.
- There is no punishment for falsely flagging free and legal speech as hate speech. This
  will permit the danger I just mentioned, as companies will have no incentive to take the
  necessary care to avoid these false flags.
- 3. Marginalized groups are more likely to be adversely impacted by this change. They will suffer the brunt of these false flags. We've seen it before. When YouTube tried similar moderation via demonetization, overwhelmingly LGBT+ focused channels found themselves being caught up in false flags. When similar legislation was passed in the United States, legal sex workers found their communication channels they used to keep each other safe damaged.
- 4. The exacting demands of the proposal will likewise ensure that only the richest of companies can afford to comply with them. If you believe in fair competition in business, then this proposal is disastrous for up and coming platforms.

For these reasons I have to urge the Candaian government to reject this proposal out of hand. The risks are too great to be worth the reward.

Thank you, Evan Sutter

Swift Peridot
ICN / DCI (PCH)
Online Content Legislation
August 11, 2021 2:58:06 PM

Canada does not own the internet. The regulation of online content should not be in any governments hands. I do not support any of the upcoming legislation, regulation, or any type of government interference in online content.

 From:
 Santiago Suarez

 To:
 ICN / DCI (PCH)

 Subject:
 This "Harmful online" laws have gone too far

 Date:
 August 11, 2021 2:33:57 PM

I'm emailing you and urged them reconsider it because it's the most dangerous approach to Canadians and the whole country. Whatever if it's a censorship or not; they can't abide it and i utterly beg you to spread the words to your citizens across Canada.

From:	Robert Rice
To:	ICN / DCI (PCH)
Subject:	Regarding the proposed harmful content regulation for social media platforms
Date:	August 11, 2021 2:32:53 PM

To the relevant parties:

This proposed internet regulation is a disaster in the making for Canadians and seems to have been written by those with no understanding of the issues behind social media platforms.

The proposed law will ensure that censorship will rule these platforms in Canada, as the proposed fines will lead companies to blanket ban any content that gets flagged for any reason, choosing to avoid the risk of the fine by simply eliminating any content that could cause trouble. This is disastrous for many marginalized communities on the social media platforms that regularly face harassment for simply existing on the platforms, including women, persons of color, the LGBTQ2S community being prominent in facing online harassment simply for having online presence.

These groups could regularly see their postings flagged for "illegal and/or harmful speech" and suffer neverending disruption from their harassers, especially given these platforms will face no consequences for removing permitted speech on a constant basis just in order to avoid fines for banned speech.

Additionally, proposed algorithms to eliminate banned speech could easily be written by these platform operators to eliminate harmless speech that they privately worry will cross a line and again, cost them money. The solution to the social media era is not to create a disastrous enforcement regime that will surely continue to gift those who thrive on targeting the vulnerable with a near-unassailable weapon to hammer them with again and again.

Also, allowing an appointed official to regularly redefine the idea of harmful content and then further to privately "advise" these services on how to avoid being targeted for non compliance of these regulations is highly disturbing. The potential for abuse in this position must not be understated, as ideology could easily influence the decisions made in this position and even a limited change to these regulations based on these decisions could have far reaching impact that could not be easily undone.

While the threat of harmful speech online will always be present, a bill that guarantees censorship, harassment and unaccountable power is definitely not the answer. I ask the government to reconsider what this bill will mean to those who will suffer the most from it.

 From:
 Matthew Sullivan

 To:
 ICN / DCI (PCH)

 Subject:
 Bill C-36

 Date:
 August 11, 2021 2:09:32 PM

Here is this citizen's input on Bill C-36:

There is no adjustment that could make this bill acceptable. Tear it up, and burn it. Never try this again. How dare you try to stomp all over our Charter right of expression like this? It makes me angry, and I am not one to anger easily. It is offensive and UN-CANADIAN. Minister Guilbeault should resign in disgrace. I am disgusted that the Prime Minister has not yet fired him from cabinet.

The current governing party has no public mandate to implement this abomination. It has lost not only my vote with C-10 and now this, but they will guarantee my active campaigning against this government until this disgraceful legislation is withdrawn. I find the official opposition party distasteful, but they can count on my vote and my support as long as they continue to oppose this bill.

Yours Sincerely, Matthew Sullivan

s.19(1)

From:	Stephen Palmateer
To:	ICN / DCI (PCH)
Subject:	comments on "harmful content" regulation
Date:	August 11, 2021 2:08:13 PM

To whom it may concern,

Many countries have proposed or passed rules similar to what is being proposed here: Australia, France, UK, Germany, India. They are all bad, but I am ashamed to say that my nation's attempt at this regulation is literally the worst.

This legislation is a worst-in-class mutation of a dangerous idea that's swept the globe, in which governments demand that hamfisted tech giants remove broad categories of speech – too swiftly for meaningful analysis.

Without detailing the horrendous elements of this regulation explicitly point-by-point [1], I'll mention that the Trudeau government is spinning these elements hard, just as they did with Bill C-10 (which included deceptive language that, on superficial examination, seemed to limit the scope of the law, but which was superseded by later clauses).

The combination of:

- prohibiting broad, poorly defined speech categories;
- · harsh penalties for underblocking; and
- requiring swift compliance without time for adequate assessment or counternotifications;

all guarantee that tech giants will block all kinds of speech.

But not all speech is equally at risk. People who are already marginalised are disproportionately likely to be censored under rules like this. Online harm rules are a human rights disaster. They've been roundly criticised by UN Rapporteurs and civil society groups all over the world [2]. France's version – which was not as extreme as Canada's – was struck down as unconstitutional [3].

The problem with Facebook isn't merely that Zuck is a shitty online emperor for three billion people – it's that no one should have the job of "online emperor." The Canadian proposal will ensure that these tech giants are the last generation of online platforms, by imposing a duty to spend hundreds of millions of dollars on speech filters – something that only the largest American companies can afford.

This regulation is a terrible vision for our online future. We don't want wise emperors running our digital world – we want to *abolish* emperors and give people the right to technological self-determination.

Best,

Steve Palmateer

[1] https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filtering-blocking-and-reporting-rules-1

[2] https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile? gId=26385

[3] https://www.eff.org/press/releases/victory-french-high-court-rules-most-hate-speech-billwould-undermine-free-expression

 
 From:
 jbash aka John Bashinski

 To:
 ICN / DCI (PCH)

 Subject:
 Comments on proposed "harmful content" regulations

 Date:
 August 11, 2021 2:00:23 PM

 Attachments:
 OpenPGP 0x8F93F16937EA588D.asc OpenPGP signature.dat

## Overall summary

Module 1 is entirely misguided, and should be discarded. If there is a replacement proposal, it should take no significant elements from this one. No central strategy of Module 1 can be repaired or salvaged.

Most of this submission addresses Module 1. Some brief comments on Module 2 are also included.

## Summary for Module 1

Every major aspect of Module 1's proposed strategy would be ineffective, actively harmful, illegal under the Canadian Charter of Human rights, and/or represent a disproportionate and unreasonable imposition on private actors for little or no public gain.

The correct response is to completely scrap what you have and start over, committing yourselves to craft a new proposal that adopts none of the existing proposal's strategies. In particular, no content-based measures are appropriate or acceptable.

One possibly productive replacement strategy would be to limit the use of "engagement promoting" designs by social media platforms, without reference to the content of the material they carry. The problem you are trying to solve is a structural one and should be addressed by structural changes, not content-based restrictions.

Unacceptable elements of Module 1

\*

 Creating the proposed legal category of "harmful" content would be inappropriate and illegal.

The "harmful" category is apparently not restricted to content which is presently illegal, or indeed to content which may be illegal in the future.

The words "The Government recognizes that there are other online harms that could also be examined and possibly addressed through future programming activities or legislative action" make it clear that this is intended to be both an open license for regulatory action to restrict speech in Canada, and a means for advocates to obtain new speech restrictions in "friendly" fora, while avoiding Parliamentary oversight and public scrutiny.

Case law in Canada has arguably gone too far in recognizing categories of content which it permits to be treated as outright illegal. It is still less appropriate to create additional, and relatively elasitc, categories of content which are "illegal on the Internet".

- a. The proposed approach could not be justified in any free and democratic society, regardless of that society's specific laws.
- c. It would be directly contrary to the letter and spirit of Section 2(b) of the Canadian Charter of Rights and Freedoms, and even more so if mere regulatory authority can be used to extend the list.
- c. Its implications would violate Section 2(d) of the charter.
- d. In reasonably foreseeable circumstances, it would be likely to cause or encourage infringements of various provisions of Sections 7, 10 and 11 of the Charter.
- 2. Regardless of (1), commanding service providers to detect harmful content content, and/or to decide whether any particular content was or might be harmful, would mostly fail to achieve its intended objectives. Even assuming, arguendo, that it did in fact achieve those objectives, it would nonetheless cause unintended harm outweighing the value of those objectives. It would also be an enormous economic burden.
  - a. It would likely be ineffective against most or all of the listed categories of content. In general, people involved with such content have incentives to find ways around blocking systems, both automated and human-operated. Furthermore, they assist each other in doing so, sharing methods that work, developing coded language, and so forth. If pushed too hard, they can simply migrate to closed, more or less explicitly illegal, platforms that are out of reach of the regulations.

On the other hand, the many people who are not significantly engaged with such content, but who would be damaged by the regime you propose to create, do not have such options or such resources.

b. The proposed regime would be certain to lead to tremendous overblocking, and that overblocking would disproportionately harm people who have and would continue have little or no power to defend themselves.

Avoiding overblocking, or processing an appeal, requires meaningful human review of the content and of the context in which it is posted. This involves close reading, evaluation of context (possibly over weeks or months and possibly including material not on the evaluting provider's platform), examination of patterns of behavior, investigation of the meaning of uncommon or "coded" language and allusions, following links, etc. This is extremely time consuming and sometimes not even possible.

The 24-hour response requirement does not allow enough time for even cursory human review, let alone meaningful review.

Because service providers would be unable to guarantee meaningful review, they would in practice be forced to block all or nearly all flagged content with no human review, or with human review so cursory as to be pointless.

Malicious actors would of course notice this and abuse the flagging system, thus further ballooning the volume of improperly flagged content and making human review even less feasible. Malicious actors would also make it impossible to rely on heuristics like a piece of content's receiving more than some threshold number of flags; they would simply raise more flags until the content came down.

None of this this is purely hypothetical. All of it, including widespread malicious abuse of flagging systems, has been seen many times in existing moderation systems on many platforms.

Many of the actors involved in creating and perpetuating the targeted content are also major abusers of flagging systems, which they weaponize against the objects of their particular hatreds. The proposal stands to damage exactly the people it purports to protect.

As an example of a failed system, YouTube, which has been relatively proactive in blocking, has caused enormous damage simply by trying to address the relatively simple problem of enforcing copyright. YouTube's copyright overblocking is so famous, and so dangerous, as to have created a pervasive climate of fear among YouTube video creators. A final "copyright strike", however unjustified, can destroy their livelihoods.

As a result, not only has material which did \*not\* violate copyright been repeatedly taken down or "demonetized", but there has been an enormous and clearly visible chilling effect preventing even the creation of a great deal of content which also would \*not\* have violated copyright.

YouTube is an extremely sophisticated, well-resourced player, and has apparently been trying to act in good faith. Deciding the copyright status of a video is trivial compared to identifying or evaluating any of the targeted classes of content. Although malicious copyright flags are fairly common, they are not nearly so common as malicious flags would be for many of the listed forms of content.

Even with enormous resources and a relatively easy problem, YouTube's copyright takedown system has been an abject failure from any perspective that considers either justice or the net social value created. Certain entertainment corporations love it, but it in fact a disaster. There is every reason to expect that, regardless of good faith, any service provider's system for the much more difficult problem of dealing with content targeted by this proposal would be an even worse failure.

c. The harms in (b) would not in practice be mitigated by requiring that an "appeal system" exist. Only a vanishingly small proportion

of appeals could possibly receive the necessary attention, and a "successful" appeal would rarely provide meaningful relief.

- i. Properly processing an appeal would involve human review, which is time consuming for the reasons described above. Even a few malicious "flaggers", or even well-meaning but overzealous ones, can easily generate far more cases than any service provider, of any size, could ever properly consider. (NB: The distinction between malicious and overzealous flaggers can also be a hard one to make).
- ii. There would be little legal or regulatory incentive for a service provider ever to sustain an appeal or even to provide genuinely meaningful review of one.
- iii. Much Internet content is only relevant for a short time after it is posted. If your content is taken down 4 hours after you post it, even if you win the "appeal lottery" and manage to get it restored weeks or months later, you have rarely received significant relief. Still less so if your entire presence on a platform has been removed for long enough that your followers have forgotten you.
- iv. Navigating an appeal process is usually extremely difficult for a person who lacks bureaucratic sophistication and/or legal sophistication, and who cannot afford to hire advisors who have them. This describes many disadvantaged persons, including many who would be likely targets both for malicious reports and for overzealous and misguided reports that could be argued to be made in "good faith".
- d. The 24-hour time limit would be so excessive that it would be likely to drive services providers to try to identify targeted content using automated means, even before it was flagged. In fact, the proposal seems to be designed to create incentives for this.

All known systems for doing this are extremely inaccurate, and most of them can be intentionally "gamed" to make them even more so. This includes all existing forms of machine learning. Decisions about the targeted types of content are difficult even for humans, and will be utterly beyond computers for at least several decades.

There is a great deal of hype around "AI" at the moment, and in fact machine learning can do some impressive things. This is not one of those things.

Attempts at automated detection will result in an additional measure of overblocking. I wish that I could say it would be random overblocking, but in fact such systems tend to reflect prejudices embedded in their training data, and therefore to systematically disfavor minorities, especially unpopular ones, as well as people and topics that might make some people uncomfortable.

e. It would be inappropriate to force private actors into the role of censor, even though they do not want that role. Furthermore, it is inappropriate to encourage large private corporations to manipulate public discourse.

The proposal does this in a particular bad way, because it subjects service providers to meaningful penalties only for underblocking, never for overblocking, and would hold them accountable only to authorities whose sole compulsory power, and likely whose sole interest in practice, would be to demand greater restriction on speech.

These unelected, and indeed unappointed and effectively conscripted, censors would be given only incentives to suppress, never to permit.

f. Even making a good faith attempt to adhere to the letter and spirit of the proposed requirements would have enormous resource and opportunity costs. Additionally trying to limit collateral damage to "non-harmful content" would present such a high cost per unit of value created that no viable business could make more than the barest token effort effort to do so.

- g. The proposal requires building (or paying others to build) complicated systems to deal with difficult problems on pain of serious penalties. The resulting costs would grossly disadvantage small and nontraditional service providers, thus concentrating and centralizing private power over communication on the Internet.
- 3. The proposed regulatory apparatus would receive an inappropriate and unacceptable delegation of Parliamentary authority over sensitive matters implicating Charter rights. This is different in kind from areas in which authority has traditionally been delegated to regulators.

It would at the same time create confusions of authority with regard to disputes traditionally and far more appropriately decided in the courts.

4. The proposed reporting requirements are unnecessary. There is, in practice, no real risk that a legitimate service provider, having actual knowledge of imminent and serious harm to anybody, would fail to make a report without compulsion. The only exception to this is the case of service providers who are themselves participating in or intentionally enabling the dangerous activity; these will not report regardless of the law.

Despite their superfluity, the reporting requirements are dangerous.

a. The most natural and convenient implementation of these requirements would be to create an easily abused semi-automated data collection apparatus with a strong tendency to over-report. This would a "single point of failure" by placing excessive trust in the constant, permanent incorruptibility of law enforcement and intelligence agencies.

- b. The requirements would invite the creation of automated surveillance systems intended to detect the targeted content. As described above, such systems are notoriously unreliable, and they would damage user privacy by subjecting non-targeted content to review by service provider staff and/or intelligence and law enforcement personnel. All users would be affected, but experience with these systems show that such burdens typically fall disproportionately on members of unpopular and/or disadvantaged minorities.
- 5. The requirements would place unacceptable limitations on new and/or uncommon technical architectures, such as decentralized peer-to-peer systems, which likely would not have any points of control at which to filter, remove, block, or preserve data. Introducing such points of control would in many cases destroy the unique advantages of these systems.

## Alternatives for Module 1

The primary source of the present-day Internet's effectiveness in spreading misinformation and propaganda appears to be the "engagement promotion" strategies favored by social media platforms. In implementation, these strategies are largely insensitive to the actual content carried, but they tend to select and amplify for the extreme, the shocking, and the divisive.

They also often tend to help users to settle into "bubbles" wherein they can form in-groups with people with whom they agree... while at the same time providing "battlegrounds" where they can emerge and harden their divisions from members of their newly created out-groups, or outright attack those they've chosen as victims.

Regulatory approaches should strike at the root of this problem by forcing platforms to change the core of the way they work, rather than by applying "patches" to disadvantage some of the content that naturally results.

Developing useful strategies for solving this would require a great deal of thought and research. I offer some suggested avenues for exploration. They are here mostly to illustrate the general direction of regulation I suggest. Some of them might not help, and indeed some might be counterproductive. There are surely many other possibilities, many of which may be be much better than these.

The complete disregard for the concerns and incentives of the advertising economy is, however, intentional.

 Invalidate and forbid all platform terms of service which prevent users from interacting with a platform's content using software other than that provided or approved by the platform itself (for example prohibitions on "screen scraping" as practiced by or on behalf of individual users).

The intent is to allow users to choose presentations which prioritize giving them the information they want to see in the ways they want to see it, over presentations which prioritize keeping them nervous, in front of the screen and engaged with the platform. This would also reduce "lock-in" and therefore have salutary effects on competition between platforms.

Forbid modifying user search results on based on past searches or on which material that particular user has chosen to view in the past.

The intent is to reduce the formation of "bubbles" by exposing users to alternative points of view.

 Prevent or restrict "home pages" or "timelines", or content suggestions from selecting material based on signifiers of controversy; such as reply rates, endorsements ("likes"), propagation ("forwards", "retweets"), etc.

The intent is to reduce platforms' promotion of controversial content, or content that contains propaganda "hooks", in the service of boosting engagement.

4. Require a time delay before a user can easily make a public endorsement of content, reply to content, or propagate content within a platform, except for the case where the propagating user personally and individually specifies every other user who will see that specific endorsement, reply, or propagated content.

The required delay should at minimum be long enough to allow the average person to read or view all of the content itself, plus one to two minutes. If the content is short, the delay should be long enough to read any featured links. If the platform can actively determine that the user has not viewed all of the content, it should not allow propagation at all.

If the reaction or propagation will reach or affect a large audience, the delay should be longer. The delay should also be lengthened if the user has already reacted to the content in question or to any of its "parent" content.

The intent is to provide time for reflection and "cool-down" before potentially damaging material is propagated, reduce misunderstandings, moderate arguments, and

5. Limit the number of separate items of content any one user may introduce in a given time. This should be done by counting the number of top-level "units" of material that are visible to other users and that compete for attention with other content, not the individual size of each one. If anything, longer texts should be encouraged over shorter ones, and including multiple images or videos under one heading should be encouraged over making each one a separate posting.

The intent is to prevent the "Gish Gallop" strategy of posting large volumes of low-quality or inaccurate content.

Forbid small limitations on the amount of text in any individual "content unit".

The intent is to encourage clear explanations and complete expositions.

 Require that platforms offering endorsements ("likes"), also offer disendorsements ("dislikes"), which effectively offset any effect of the endorsements in content selection.

The intent is to make "brigading" less productive.

 Do not permit users to control other users' views of the replies or reactions to their content, unless those other users have explicitly opted into that particular user's control.

The intent is to prevent creating spaces of false consensus.

Forbid targeting advertising based on anything other than the content the user is presently viewing.

The intent is to reduce the use of targeted advertising as a propaganda vehicle.

#### Module 2

Module 2 contains some unobjectionable and even desirable parts, such as centralized reporting.

The 12-month preservation requirement for the Mandatory Reporting Act seems to include preserving the actual child pornography itself (and I assume that there's a provision somewhere making that legal). Although a large service provider might have no problem complying, I could imagine that a small one would have trouble properly securing "radioactive" content such as child pornography for 12 months. Perhaps the requirement should be changed to require transmitting the actual child pornography, without any metadata, to NCECC as part of the actual report, then deleting that locally, and preserving only other related data.

The main thrust seems to be providing more subscriber information to law enforcement and intelligence agencies. This may have undesirable elements.

It seems likely that by now law enforcement has probably learned not to overinterpret BSI, but it seems a bit unwise to automatically give anyone, including law enforcement, information about recipients ("destinations") of child pornography, unless there is evidence that they have knowingly solicited it (and perhaps actually received it). And that evidence should probably be evaluated by a court.

I'm prepared to believe that CSIS should have the same BSI access as law enforcement, but am a bit mystified as to how they could properly use it, given that they would still need another order to actually initiate surveillance based on it, and that using it to build a "social graph" would be both unreliable and, I suspect, illegal.

From:	Yoonsik Park
To:	ICN / DCI (PCH)
Subject:	Concerning Language, Discrimination against Small Communities
Date:	August 11, 2021 1:55:30 PM

### Hello,

I have two main concerns with the rules from the "proposed approach to address harmful content online".

Concern 1:

I am surprised by the language given in section 1(B) 17 of the technical paper. This gives immense leeway to the Digital Safety Commissioner in regulatory decisions, and creates a situation where certain OCSs or OCSPs may be given special privileges. Furthermore, it causes unnecessary ambiguity to companies or services that are being created, causing a chilling effect on startups and new social media companies. Canada is leading in tech innovation, and laws like these will inhibit the growth. I believe there are healthier options than allowing arbitrary "tailoring" of regulations. These rules need to be codified in law, and should take a minimalist approach.

Concern 2:

As we see the growth of "big tech" platforms, I agree many problems are linked to inadequate moderation. However, this proposal does not address the success of small online platforms with good moderation. Personally, I believe that small communities, i.e. federated social media platforms, such as "Mastodon", will rise up to fill the niche of small moderated platforms. The size of these platforms is directly linked to unwanted behaviour. You can see the success of small communities on the site "Reddit" with an amazing number of high-quality "subreddits". Due to the accessibility of tech, people are now starting the equivalent of their own "subreddit" on their own servers with "Mastodon". We should see a clause allowing broad exemption from these rules when under a certain limit, such as number of active users.

Also, this proposal could be seen as a form of discrimination against a rural municipality trying to start their own online community. The concept of "small online community" must urgently be addressed.

Sincerely,

Yoonsik Park

 From:
 Lyle Button

 To:
 ICN / DCI (PCH)

 Subject:
 Proposed Harmful Content Bill

 Date:
 August 11, 2021 1:46:25 PM

I have read the online harmful content proposal. Please drop this initiative entirely. Democratic governments should not resort to dictatorial control of communications no matter how much they admire the governments that do so.

I find it ironic that our federal government considers it essential to limit harmful speech, such as you might expect to be directed at Muslims, for example, while at the same time doing nothing to protect Canadian Muslims in Quebec from active discrimination by that government.

Thanks,

Lyle Button

s.19(1)

From:	Steve T (ACCESS 10	
To:	ICN / DCI (PCH)	
Subject:	Tech worker response to the proposed approach to addressing harmful content online.	
Date:	August 11, 2021 1:03:46 PM	

Hello and good day,

I'm a UX designer from Vancouver, one of Canada's major tech hubs. I spend time everyday weighing ethical issues and trying to balance the intent of my team against the effect it has on real people and I believe this proposed approach completely misses the mark on making the internet healthier in practice for Canadians.

One of the greatest faliures of this approach is that this legislation, aimed to be representative of the Canadian people's interests, entirely puts the responsibility on regulated entities to comply within legislation, but these entities rarely have the collective good of the Canadian people in mind. The discussion goes so far as to mentions the use of automated systems and algorithms as a potential tool of use by these entities for flagging and reporting content. Not only are these algorithms already demonstrated to be prone to racism, the need for these robust systems would more deeply entrench tech monarchies that can afford them. I am all for regulated social platforms and ideally breaking up tech monopolies, but this approach would guarantee that only massively wealthy online platforms can play. This approach does nothing to speak to the systemic racism and misogyny that these platforms reinforce as they operate.

Secondly, this approach deeply dives into content, reporting, and appealing without also grappling with the fact that these functions, these user actions, are powerful tools that hate groups and terrorist groups already use to harm indigenous, queer, and marginalized creators. I have no faith in these tech entities that their appeal processes would be fair or just. An reporting and appeal process for online content is incredibly expensive, so corners will be cut without doubt at the harm of Canadians. This type of legislation has been seen on other countries and the results are bleak and often unconstitutional (like in France for example). In practice this approach could block consensual sex workers from operating online which greatly impacts their safety and well-being. In practice this approach will see large social platforms continue their often unethical work as normal while leaving the safety of vulnerable people to an automated system. This approach would see new, potentially better, entities indirectly prohibited from operating in Canada while Facebook and pornhub continue to wreak havoc. This bill would see extremist groups armed with a deadlier reporting tool for harassing vulnerable people.

Most importantly, the unclear wording of this is ripe for misuse, especially as the ability to change these definitions while enforcing them is private. I shudder to think how this position could be abused if a Doug Ford type were to be appointed.

I've worked in this field. I've seen how platforms deal with this kind of legislation. I call on you to toss out this approach and come back with something that gives sex workers, indigenous groups, children, and marginalized groups more rights and protections online under the law.

Thank you for your time, Stephen Therriault

UX designer, Concerned Canadian

From:	Jon Babyn ME ACCESS TO INT
To:	ICN / DCI (PCH)
Subject:	The Government's proposed approach to address harmful content online is not the right one!
Date:	August 11, 2021 1:02:57 PM

Giving the Canadian government more powers to spy on Canadian citizens for vague terms like terrorism is outright terrifying. This is not the right approach and could easily have disastrous consequences if abused. With vague terms like terrorism an authoritarian leaning government could use this act to silence political dissidents online.

Blocking swaths of the internet is also an approach that has been shown time and time again not to work. Determined people find ways around or alternative methods to spread their message.

The government should be focusing efforts on improving digital privacy, access to the internet and improving the rights of consumers of digital services not making it worse.

Regards,

Jonathan Babyn

From:	Grant Longhurst
To:	ICN / DCI (PCH)
Subject:	Harmful content legislation and regulation
Date:	August 11, 2021 12:47:53 PM

This is an appalling restriction of free speech, and the entire proposed approach needs to be scrapped.

- It will prohibit overly broad, poorly defined speech categories
- Impose harsh penalties, while at the same time requiring compliance without time for adequate assessment
- And all but guarantees that Charter protected kinds of speech will be blocked with no recourse.

And who in the world thought having a politically appointed "internet czar" was a good idea. And mandatory reporting of *potential* harm? For goodness sake, stop this now.

Grant Longhurst Direct: 604.506.2445

High Performance Communications Inc. 220 – 145 Chadwick Crt North Vancouver BC V7M 3K1 www.highpci.com

From:	a@arbastrategies.com a@arbastrategies.com
To:	ICN / DCI (PCH)
Subject:	the harmful content law is awful
Date:	August 11, 2021 12:32:15 PM

Sometimes the best intentions lead to the worst ideas. And that's what happened with this proposed legislation. It is overreach and instead of protecting vulnerable communities it will end up hurting the very communities it seeks to protect. C-10 was bad enough. This is worse. We have evidence of what these laws end up doing from all over the world. The government seems to have learned nothing from overseas.

Arjun Basu President

<u>arba</u>Strategies

a@arhastrategies.com 514-813-0630 @arbastrategies

From:	Josh Friesen
To:	ICN / DCI (PCH)
Subject:	Concern
Date:	August 11, 2021 12:25:18 PM

# Hi,

I am concerned about the proposed Bill to regulate internet content. Particularly the 24 hour window that companies are required to take "potentially" harmful content down, which will inevitably result in big companies taking a broad approach to censorship, as they wont be penalized if they get it wrong and censor something that wasn't harmful. I'm also concerned about the requirement to report any "potentially" harmful content to the police. While I dont think this will be abused by the liberals, it's not hard to see how this could snowball if the next government is far-right. Hate speech and misinformation does need to be addressed on the internet, but this is not the way to do it. Give tech companies more time to thoughtfully process information and hold them accountable if they take something down incorrectly. Only illegal behavior should get reported to the police. This bill is irresponsible.

Thank you,

Josh Friesen

 From:
 Dana F.

 To:
 ICN / DCI (PCH)

 Subject:
 This legislation does not address the underlying issues

 Date:
 August 11, 2021 11:19:25 AM

If this legislation passes we are headed towards a Chinese-style firewall/censorship. It would not have prevented the more harmful use of internet expression, the most prominent examples being Trump and Bolsonaro's use of social media to convince voters to back their campaigns through lies and misinformation. It will not prevent Russia from doing the same with our politics.

Finally all the ISPs and major social media sites will simply start overbanning, due to the threat of fines and other legal action, and kneecap the internet as the premier nexus for idea exploration and sharing views that unite us as humans.

Thanks, Dana

From:	Jeffrey Cliff
To:	ICN / DCI (PCH)
Subject:	The Government's proposed approach to address "harmful content online"
Date:	August 11, 2021 11:12:59 AM

The "Online Harms" proposal, as written, is not fit for what should be a free society and should be completely scrapped. And everyone involved in pushing it *should immediately resign in disgrace*. The harm you will do this country by pushing it to law will be vast, and will undermine the very foundations of this country.

Any of you bureaucrats reading this email, who allow it to continue to progress - we will find your names, and history will remember how you stood when the basic fabric of our country was threatened.

Jeff Cliff

End the campaign to Cancel Richard Stallman - go to stallmansupport.org !

s.19(1)

 From:
 Don Cameron

 To:
 ICN / DCI (PCH)

 Subject:
 Address harmful content online

 Date:
 August 11, 2021 10:42:49 AM

This entire initiative is totally misguided and misspent effort. In medicine, whether you are a good doctor or not depends on whether you treat symptoms or patient health; they are not the same! In treating patient health, root causes need to be identified and addressed.

Things like a failed education system that overly burdens educators and does not care about teaching knowledge, empathy, and respectful discourse, but rather focuses on test scores and credentialism is a root cause.

Stop trying to treat symptoms! Focus legislative effort on root causes. Police criminal acts in the real world. Be better than implementing a system that turns authoritarian at the flick of a switch.

From:	Frank.Brown ME ADDESS	U
To:	ICN / DCI (PCH)	
Subject:	(No Subject)The Government's proposed approach to address harmful content online	
Date:	August 11, 2021 9:59:39 AM	

Greetings,

After having read through this technical paper, I am not in favour of it being implemented as law for the following reasons:

1) existing laws already cover this issue.

2) it is technically problematic to require service providers to remove content within the timeframe provided.

 this kind of proposed legislation can be used to restrict free discussion for political purposes.

4) this restricts free speech.

5) this will provide incentive to drive the content at issue underground to a dark web, etc where it can exist outside the reach of existing laws and law enforcement.

6) this is not a canadian heritage issue.

Regards,

Frank Brown

s.19(1)

Graeme Chandler
ICN / DCI (PCH)
Online Harms Proposition
August 11, 2021 9:41:30 AM

I have several extremely serious concerns regarding many of the ideas put forward in this proposal, not the least of which is because the Criminal Code of Canada already accounts for ways to deal with issues related to online exploitation.

Firstly, website blocking is an outdated concept that doesn't work. People and providers just navigate to a new domain, and the entire thing becomes a costly game of whack-a-mole for tax payers.

Harmful speech that is legal but potentially offensive or upsetting has issues around subjectivity, but even more so when it comes to online material. For example, given the current issue around Residential Schools, putting a mechanism in place to catch discriminatory material aimed at Indigenous Canadians has a very high risk of also catching material from survivors of Residential Schools, as they both can contain similar subject matter, but are different in intent. When held up to scrutiny, there is no existing (or likely existing) automated system that is able to distinguish between the two, as context is something that requires human review. This may sound nuanced or trivial, but it has resulted in YouTube effectively stopping all mention of events like the Holocaust on their website, as the automated review lumps it in with antisemetic material. The alternative is that they risk allowing hateful material onto their website, but rather than treat the situation fairly, they prefer to scrub it entirely so they don't have to deal with it. You are in effect taking that model and applying it to the rest of the internet for Canadians, which, in this example, would result in every website shutting down any mention of Residential Schools to prevent a risk of being fined by the government for falling afoul of this legislation.

Demanding that any platform remove content within 24hrs is absurd, as it requires websites to input a general monitoring scheme to have even the slightest chance to comply. Such a system is, by nature, prone to false positives, as you are demanding that a machine understand the concept of things like sarcasm and pastiche, which it simply cannot and will not be able to do regardless of how advanced it is. Human review is mandatory, which is not something that any website outside of the largest American platforms have access to, and even then at a very compromised degree. Additionally, in my experience, most of these measures do not even work to begin with, as I still am able to run into explicitly pornographic material on YouTube on a regular basis. Whatever you are envisioning to deal with this problem is only going to create a headache for general Canadians, and showcases a serious lack of understanding in the capabilities of existing and future technology.

I could go on, but the reality is that there are portions of this legislation that are worded in a way that conflicts with the Charter of Rights and Freedoms, and will not hold up to legal scrutiny. If you are really interested in protecting Canadians from online exploitation, this is the worst way to go about doing it, as it will not accomplish the original goal in the slightest.

We are in a pandemic and a probable election year. As a registered voter, I have a right to demand that you do better than this.

Thank you very much,

-Graeme

From:	Greg C.
To:	ICN / DCI (PCH)
Subject:	Feedback - Online Harms Bill
Date:	August 11, 2021 9:29:22 AM

I have several concerns regarding this proposal, and do not support this being implemented.

Most concerning is the lack of judicial input on what content is to be permitted / blocked. Definitely do not trust an agency to decide what is or is not acceptable - THAT is why we have Courts.

Also of concern is the act first, decide if the content is valid later... that is guilty before proven. If the content is grossly illegal, then a judge panel will take no time to create a takedown order. If there is ANY question as to the legality of posting - according to existing laws - then put the matter to a judge panel.

In no way should providers, or an agency, be compelled to respond to a complaint first and put it to the court later. That is just censorship at the hands of ANYONE who writes a complaint.

Complaints must be made public, with accuser and accused and complaint shared publicly. Context is important, and motives must be assessed for any complaint.

IN short... take nothing down without judicial control.... beyond current exploitation laws.

Regards, Greg Crowley

From:	Daniel Ralston
To:	ICN / DCI (PCH)
Subject:	Handling "Harmful Content" Online
Date:	August 11, 2021 2:00:46 AM

## Hello,

I fully and strongly oppose the entirety of the government's proposed approach for handling "harmful online content".

The current consultation is not a consultation at all. It has been brought almost to full completion without any consultation of the Canadian people, in direct opposition to the Liberal promise to increase consultation and transparency. As the proposed legislative changes have been completed before consulting the Canadian people, there is now no room to craft a system centered around the expressed wishes of Canadians. This "consultation" is a statement of the government's intentions, not an opportunity for Canadians to take part in the ground-level construction and goals of this proposed system. This proposal, exposed only after finishing it in back-room talks, is an affront to Canada's system of representative government and I will not stand for it.

The system is also massively biased in favour of offhand censorship. A 24-hour review of a complaint cannot reasonably be performed. No company on the planet has the human resources to ensure that unfair complaints are discarded. Therefore, one online complaint will be enough to remove any speech that anyone, anywhere disagrees with. Such heavy-handed censorship would be considered extreme for even a repressive country — in those countries, only the government has a blank check to censor whatever they please. This proposed system would give that same power of repressive censorship to anyone by making it effectively impossible to ensure fairness.

It is already too hard to have honest and respectful discourse anymore. Extremists on both sides take violent offense to anyone who disagrees with them. Don't make the horrible divisions in our country worse by allowing anyone to censor anyone else. Speech must be free.

No one is "harmed" by hearing speech they don't agree with. If that was so, this affront to freedom of expression from my own government would certainly have hurt me.

This proposal is un-Canadian and an affront to freedom of expression. The UN human Rights commission has denounced less extreme proposals from other countries such as Germany.

Let Canadians tell you their priorities, then build a system based on what Canadians want from the ground up. Scrap this oppressive affront to freedom of expression that you've cooked up behind closed doors.

I am tired of having to fight censorship and threats to freedom on my own soil. Canada deserves better.

Daniel Ralston Canadian Citizen

From:	June Sapara
To:	ICN / DCI (PCH)
Subject:	Harmful content online
Date:	August 10, 2021 11:33:19 PM

This proposal has been called to the worst of all the G20 laws for online content and free speech.

This sums it up well.

https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filteringblocking-and-reporting-rules-1

Please stop, respect free speech and privacy. Our democracy depends on it.

June

Thomas Tulk
ICN / DCI (PCH)
digital citizen initiative feedback
August 10, 2021 11:31:49 PM

Sorry if this comes off as blunt, but it looks mostly like a load of spying and censorship trash to me, pal. Are there not already laws on the books that can be applied to these situations? I get that you've got limited options for trying to address these kinds of problems, and you're probably initially suggesting this kind of big blunt-instrument approach fully expecting to be talked down into something less embarrassing, fine.

Let me get carried away for a moment, here. When I was a kid, they had a nice person with a puppet and a picture-book come to my school and warn us not to trust people because people are sometimes out to "hurt kids", and that you should always fight, scream, run away and talk to trusted adults if anyone hurts you or tries any tricks on you. There was a bit of euphemism involved at the time. Do people not teach children not to trust strangers anymore? That you definitely extra cannot trust internet strangers? If you want to help people with this kind of thing, enable the citizenry to live better lives, maybe. Used to be a husband's pay might feed and raise a big family. Now both parents have to be working long hours all week to make ends meet just to raise one or two kids, if the kids are lucky enough to even have both parents, and there's barely anyone left to raise or supervise them. They're letting their babies use internet-connected ipads unsupervised. A web-connected communications device isn't a baby's toy or a babysitter! Sometimes they find this out the hard way when the kid wastes a load of their money buying game coins. Try addressing these base-level problems by HELPING PEOPLE and TEACHING PEOPLE and you're well on your way to cutting down on the kind of thing you're trying to solve backwards with your top-down surveillance state-in-the-making junk.

From:	Chris Berdych
To:	ICN / DCI (PCH)
Subject:	Disappointed Canadian
Date:	August 10, 2021 10:27:06 PM

Disappointingly, you'r short page describing how Canada is taking steps to rain in hate speech another negative online expression is woefully short on actual description of how the process occur. I had to read Electronic frontier foundation document do you understand anything about what is actually planned how it is planned to be executed.

https://www.eff.org/deeplinks/2021/08/o-no-canada-fast-moving-proposal-creates-filteringblocking-and-reporting-rules-1

It suggests that there is nothing simple whatsoever about how to go about this prescribed aim. I'm most concerned proposals will not satisfy the following agreement:

Article 19 of the International Covenant on Civil and Political Rights allows states to limit freedom of expression under select circumstances, provided they comply with a three-step test: be prescribed by law; have legitimate aim; and be necessary and proportionate. Limitations must also be interpreted and applied narrowly.

Please follow article 19"s general intent. I sincerely want Canadian government to stand as a shining example to other countries.

Chris Berdych

From:	Mike Sollanych
To:	ICN / DCI (PCH)
Subject:	Re: harmful content online
Date:	August 10, 2021 10:07:58 PM

Once again, we see the rise of authoritarianism, cloaked behind "won't someone think of the children" and other such excuses. Now, it brings with it a new wave of censorship and oppression, designed to ensure that people can only speak the correct opinions about the issues of the day.

I find the proposed legislation offensive at its core. I do not need protection from "harmful content", and I do not find it acceptable that anyone should be appointed as judge over what I am allowed to see, read, say, or think in a country that prides itself on having rights and freedoms protecting precisely these abilities.

You know as well as anyone else that what you are doing will not actually work. People who feel wronged by their government will continue to find avenues to discuss this; people who participate in the abuse of children will continue to do so. All that will be gained is more authoritarian control over our lives by a government that continually overreaches its bounds in the name of "protecting people".

Protect me from yourself.

Take your proposed legislation and burn it, and find something more meaningful to do with your petty life than to destroy the very rights that so many people died to earn and retain for Canadians.

 From:
 Shannnyn Dowsett

 To:
 ICN / DCI (PCH)

 Subject:
 Re: proposal of online content regulation.

 Date:
 August 10, 2021 10:04:18 PM

Hello,

I appreciate the effort to moderate online use as we have seen a rise in abuse and misinformation, however these proposed controls seem to infringe on free speech. Beyond that they specifically hurt smaller businesses not able to build complicated algorithms or employ lawyers to constantly moderate and ensure they are meeting standards. It takes personal responsibility off of the user and puts onus on businesses. The target is on large social media but they will have the resources to both work with and fight this. Small businesses will suffer.

It will be easier to also target say someone who makes a joke and does not seem to allow for the nuance of conversation to be understood. It will be easy to have this take down legitimate posts that are trying to expose violence or inequality.

Overall I am not satisfied with this proposal and find the potential for misuse too high.

I do not support it in its current draft.

Thank you

Shannyn Dowsett

Canada

s.19(1)

s.19(1)

 From:
 Paul Bedard

 To:
 ICN / DCI (PCH)

 Subject:
 Fwd: Harmful content on line

 Date:
 August 10, 2021 9:46:24 PM

Sent from my iPhone

Begin forwarded message:

From: Dale&Marlayne Miner < Date: August 10, 2021 at 9:27:35 PM EDT To: 1 Subject: Fwd: Harmful content on line

Sent from my iPad

Begin forwarded message:

From: Dale&Marlayne Miner < Date: August 10, 2021 at 9:22:45 PM EDT To: pch.icn-dci.pch@canada.ca Cc: charlie.angus@parl.gc.ca Subject: Harmful content on line

I am encouraged to see that the government of Canada is looking into the pornography epidemic in our country that is physically and mentally effecting our youth. I would like to see legislation that is law in some other countries where it is a criminal offence to distribute porn on line to a minor. Also I would like to see a law passed where a person of legal age who purchases a cell phone would have the option from the seller if he or she could or could not access pornography from their internet server.I would like to share with you a study from The American Academy of Pediactrics in 2008. " The availability of extreme to hardcore pornography among young children has produced within them thought processes and emotional instability with damaging effects. The emotional and mental trauma experienced is that similar to or exactly as children who have been sexually abused from a young age. There is a direct correlation between sexual abuse and pornography among the young. Studies show that the resulting effects have the same outcome, that there is an overwhelming emotional detachment from normal sexual behaviour due to their earlier

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

abuses." This committee needs to take a hard look and see what a Information Act huge negative effect pornography is having on Canada's younger generation. Please do the right thing and recommend laws that will protect their young minds. Regards, Dale Miner Sent from my iPad

From:	Lisa C
To:	ICN / DCI (PCH)
Subject:	Online harms legislation
Date:	August 10, 2021 9:43:02 PM

I do not support this. Listen to Michael Geist please.

I understand you mean well. However this seems incredibly sloppy and broad legislation. As a general rule, governments shouldn't give themselves power they wouldn't give to someone with an opposing view. I would not give this broad power to someone who held opposite views from me on what content should be restricted.

Additionally, clearly the online companies will find it easiest to take a "when in doubt, remove it" approach. I don't see any way you will be able to avoid these removals being taken too far by the companies, even if you are starting with non-overly-broad intentions.

Lisa Chamney

s.19(1)

 From:
 Peter Gillespie

 To:
 ICN / DCI (PCH)

 Subject:
 STRONGLY OPPOSED TO YOUR CENSORSHIP BILL

 Date:
 August 10, 2021 9:40:57 PM

Your proposed bill is dangerous for Canada.

It is yet another step in the direction of technological authoritarianism.

It provides a switch that allows the political class to control the people who elected it.

Today "terrorism", "child pornography", "hate speech".

Tomorrow "misinformation", "objectionable content", "anything else inconvenient".

This bill lays the infrastructure to oppress the Canadian population via a sprawling technology infrastructure serving no purpose but to advance the agenda of those in power.

China looks downright honest and forthcoming compared to the disingenuous evil embedded in this bill. At least they state openly and clearly all communication will be censored by the state.

A dark day for Canada.

Shame on you all.

 From:
 Nathan Schuetz

 To:
 ICN / DCI (PCH)

 Subject:
 Harmful content online proposal is dangerous

 Date:
 August 10, 2021 9:26:23 PM

The proposal is dangerous and should be scrapped. Automated systems are buggy but will be required for compliance, which will lead to censorship, much of it accidental. It will marginalize people. It also adds a massive regulatory burden to small tech companies who simply want to let users submit content and collaborate with one another - it will effectively ban small online businesses of this sort, but leave big tech untouched since they have massive engineering teams.

Please abandon this.

From:	Dale&Marlayne Miner
To:	ICN / DCI (PCH)
Cc:	charlie.angus@parl.gc.ca
Subject:	Harmful content on line
Date:	August 10, 2021 9:22:53 PM

s.19(1)

I am encouraged to see that the government of Canada is looking into the pornography epidemic in our country mat is physically and mentally effecting our youth. I would like to see legislation that is law in some other countries where it is a criminal offence to distribute porn on line to a minor. Also I would like to see a law passed where a person of legal age who purchases a cell phone would have the option from the seller if he or she could or could not access pornography from their internet server. I would like to share with you a study from The American Academy of Pediactrics in 2008. " The availability of extreme to hardcore pornography among young children has produced within them thought processes and emotional instability with damaging effects. The emotional and mental trauma experienced is that similar to or exactly as children who have been sexually abused from a young age. There is a direct correlation between sexual abuse and pornography among the young. Studies show that the resulting effects have the same outcome, that there is an overwhelming emotional detachment from normal sexual behaviour due to their earlier abuses." This committee needs to take a hard look and see what a huge negative effect pornography is having on Canada's younger generation. Please do the right thing and recommend laws that will protect their young minds.

Regards, Dale Miner Sent from my iPad

s.19(1)

From:	(he.A)
To:	ICN / DCI (PCH)
Subject:	The Government's proposed approach to address harmful content online
Date:	August 10, 2021 9:02:10 PM
Attachments:	Technical paper comments.pdf

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St Gatineau QC K1A 0S5

Via EMAIL: pch.icn-dci.pch@canada.ca 10 August 2021

I am writing to offer comment on the proposed approach. Thank you for this opportunity.

Comment 1 – Web 3.0: The document fails to recognize the existence of Web 3.0 blockchain driven services and how they may be used to elude Canadian law and government oversight. Earlier this year Dfinity.org launched "The Internet Computer (IC)", a platform that allows for the creation of social media platforms and other applications leveraging the blockchain. The IC has nodes around the world at unknown locations. It makes innovative use of cryptography to ensure integrity of the platform and provide censorship resistance. The platform is intended to become a competitor to major cloud service providers (Google, AWS, Azure, etc).

In order to run an application on the platform, one only has to pay for the service to run. There is no contract, and once an application launches, it cannot easily be stopped by any entity. It is possible to write code to re-instantiate the application dynamically. Essentially trying to stop the program it would become a whack-a-mole game. There is no company to which a lawful entity could make timely representation to seek injunctive relief.

Comment 2: - Web 3.0 Self Sovereign Identity: The IC has enabled Self-Sovereign Identity. A person generates securely their own identification credentials and then can sign-up to different services which cannot be cross-referenced. Each service creates a separate access token that is not shared between services. While innovative, it makes it extremely difficult to attribute who is generating traffic that falls within the five categories identified in the paper.

Comment 3: Moving beyond regulating Individuals and Corporations is necessary. New applications on the Blockchain are now emerging that leverage a governance structure called a Decentralized Administrative Organization (DAO). Once a person or identifiable entity develops an application, they can transfer ownership and control to a DAO that does not exist in law, is not a corporation, and yet is capable of exerting control over its social media platform. DAO members must use the non-attributable Self-Sovereign Identity to vote.

Comment 4: Entering a premise to look at content. New Blockchain based apps are all done online. There is no one to visit and no records to see. Seems a little archaic.

Comment5 – Liquid Democracy. Dfinity has implemented an automated governance system called the Network Nervous System (NNS), whereby token holders are able to vote on issues such as adding and removing nodes, increasing rewards, and changing services. This is done algorithmically and creates Liquid Democracy. Similarly, the Service Nervous System (SNS) is being implemented to provide a similar voting mechanism for applications whereby a proposal can be put forward for vote. I have suggested that the Dfinity NNS be capable of communicating with the SNS to advise that a complaint has been received in one of the 5 categories. Ideally, the SNS governance should kick in and present a proposal to voters of the DAO (e.g. Take down offensive comments) and respond back to the NNS saying completed or opposed.

The challenge is that the DAO may be a mix of persons from jurisdictions whose laws are different than those in Canada. The NNS, is operated by Dfinity out of Switzerland.

The Technical Document is based on a premise of centrally controlled social media. This is shifting. Distrikt and Dscvr are two examples of decentralized social media.

### Document communique en vertu de la Loi sur l'accès à l'information. Document released pursuant to

Comment 6: Unclear jurisdictions. It is unclear which law applies to a platform that is launched on the IC. The creator may not be identifiable, the location of the platform may be unidentifiable, and yet it may contain content that is harmful in the eyes of Canadians.

Comment 7. Web 3.0 enables the creation of decentralized social media. It has the potential to move platforms away from big tech. If the intention is to have OCS providers foot the cost for this oversight infrastructure, it will stifle decentralized social media as it does not have a revenue stream like big tech has. This will thwart the innovation and entrepreneurship that can is about to emerge with Web 3.0.

#### Suggestions:

 DAOs are here to stay. If a Canadian is a member of a DAO and they are aware of content that is harmful they should be required to doing something: vote to remove it and/or report it depending on a threshold.

2. Identifying Canadian ownership of an app is difficult. If an application is created and operated by a Canadian corporation or legal entity, it should be required to display this fact at the User Interface layer and at the API layer. It will make it easier to find to whom a platform belongs.

3. Any Canadian building a social media platform must be required to build in algorithmic capability to remove content contrary to Canadian law.

 Any Canadian deploying smart contracts should be required to declare the legal jurisdiction for dispute resolution in the api and in the user interface.

5. Transnational crime and unscrupulous individuals will use the legislative vacuum to their advantage. I believe G20 nations need to establish similar mechanisms and enable collaboration.

6. There are a number of committees and governance bodies. It is top heavy and not efficient.

The use of DAO self-moderation and demonstration thereof should be sufficient to meet the needs of active content monitoring.

 The Technical Document should include API requirements that Social Media OCS providers must implement (not tied to a technology).to facilitate timely responses.

I am available to discuss via video should you wish.

Ted Reinhardt

s.19(1)

Ref: dfinity.org

From:	Ice (/) E .
To:	ICN / DCI (PCH)
Subject:	Proposal to Regulate Social Media and Combat Harmful Online Content
Date:	August 10, 2021 9:01:27 PM

### Hello Digital Citizen Initiative

This message is in regards to my opposition to the Canadian Government's proposed approach to regulate social media and combat harmful online content. There are a large number of flaws in the current approach that are included in the proposal which make it unpalatable and more likely, harmful to many minority Canadian internet users, be they POC or LGBTQ\*. Examples of this can clearly be seen in the United States, following the implementation of FOSTA-SESTA in 2018. Furthermore, it could be used to assist in creating an environment where movements such as Black Lives Matter and Me Too would never have gained the traction to enact change.

The broad definition of "Harmful content," which includes legs speech, combined with the 24 hour take down requirements would result in mass takedowns of lawful content, as the short window will not provide sufficient time for reasonable consideration, taking context into account. Proposed laws in the United States which had a 72 hour take down requirement were rejected, as this was considered unreasonable as well.

The mandatory reporting of potentially harmful content, and about users who post it, would capture broad swatches of content being reported to law enforcement, which would only burden them in sorting through perfectly legal content from those small amounts that are not. The data retention requirements are also unreasonable, requiring those required to do so, to devote vastly increased resources to complying with this.

The possibility of website blocking is arguably the worst aspect, creating a possible vehicle for state censorship based on the political party wielding the post power at the moment, and is a policy most at home in China or North Korea, than a nation that is seen as a global leader in freedom and democracy.

Overall, this proposal is dangerous to internet speech, privacy and the security of Canadians.

Regards

Hayden Polski

From:	s.19(1) the Access to Information
To:	ICN / DCI (PCH); Steven.Guilbeault@parl.gc.ca; Prime Minister of Canada; chrystia.freeland.c1b@parl.gc.ca
Cc:	Justin.trudeau@parl.gc.ca; chrystia.freeland.c1b@parl.gc.ca; Anita.Anand@parl.gc.ca;
Set 126.0	carolyn.bennett@parl.gc.ca; Marie-Claude.Bibeau@parl.gc.ca; Bill.Blair@parl.gc.ca; Bardish.Chagger@parl.gc.ca;
	Francois-Philippe.Champagne@parl.gc.ca; jean-yves.duclos@parl.gc.ca; Mona.Fortier@parl.gc.ca;
	marc.garneau@parl.gc.ca; karina.gould@parl.gc.ca; Steven.Gullbeault@parl.gc.ca; Patty.Hajdu@parl.gc.ca;
	Ahmed.Hussen@parl.gc.ca; melanie.joly@parl.gc.ca; Bernadette.Jordan@parl.gc.ca; Lametti, David (Ext.);
	dominic.leblanc@parl.gc.ca; Diane.Lebouthillier@parl.gc.ca; lawrence.macaulay@parl.gc.ca;
	Catherine.McKenna@parl.gc.ca; marco.mendicino@parl.gc.ca; Marc.Miller@parl.gc.ca;
	Maryam.Monsef@parl.gc.ca; joyce.murray@parl.gc.ca; Mary.Ng@parl.gc.ca; Seamus.ORegan@parl.gc.ca;
	Carla.Qualtrough@parl.gc.ca; pablo.rodriguez@parl.gc.ca; Harjit.Sajjan@parl.gc.ca; deb.schulte@parl.gc.ca;
	Filomena.Tassi@parl.gc.ca; Dan.Vandal@parl.gc.ca; Jonathan.Wilkinson@parl.gc.ca
Subject:	Response to limiting Cdn. free speech
Date:	August 10, 2021 3:47:21 PM

August 10, 2021 Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St Gatineau QC K1A 0S5 Email <u>pch.icn-dci.pch@canada.ca</u> Telephone 819-997-0055

Under the cover of child porn legislation, your government is proposing to eliminate political expression which it could choose to label "terrorist content, incitements to violence and hate speech". The government's real target in your background material is described as: "Online Ideologically-Motivated Violent Extremist communities [that] range in the tens of thousands, acting as echo chambers of hate for adherents from all over the world". While this might be taken to apply to Israeli settlers and their supporters or even to Trump's people, it is obviously meant to be understood as Muslim organizations, particularly with its use of capital letters indicating a specific target. This is implicitly Islamophobic racism and it is unacceptable. (Our family is not Muslim but we object to all racism, and this appears to be racist.)

This legislation threatens —and can eliminate— Charter freedom of expression when legitimate information fits what the pro-Israel lobby, supported by your government, might designate as:

- "terrorist content" [which might be claimed to include: information that supports the popular, nationalist political parties Hamas or Hezbollah or mainstream Iranian or Yemeni or Syrian nationalists or exposes terrorism involving Israel or its agents];
- "incitements to violence" [which might include descriptions of Israeli criminality in its ethnic cleansing, terrorism and genocide of Palestinians or other terrorism supported by the Canadian government] or
- "hate speech" [descriptions of Israeli racism and criminality or of the pro-Israel lobby's subversions of Canadian democratic values and freedoms].

The Canadian Heritage Ministry's proposed legislation appears to fit B'nai Brith's wish list for on-line content control, namely the resurrection of the hate speech legislation [that seems to be defined only as anti-Jewish] along with the ability not only to eliminate content describing Israel's racist crimes against Palestinians but also to have CSIS identify sources. This is not only censorship, it is intimidation. It appears to be the pro-Israel lobby's follow-

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

up to the passage of the IHRA definition of antisemitism which threatens information about Act describing the Palestinian situation at the expense of Canadian freedom of speech/expression.

We want a harmonious society without any racism or discrimination, and we believe that the Charter right to freedom of expression is not a privilege <u>but our right</u>. We believe that this proposed legislation reinforces Islamophobic racism while threatening our freedom of speech. Many of us, moreover, believe that Canadians of conscience have a moral imperative to speak out on the situation facing Palestinians, particularly because your government is supporting Israel's crimes against humanity while ignoring its contractual legal obligation under the Fourth Geneva Convention to protect Palestinian rights.

We are also upset that this feedback period ends before people return from summer vacations: many will not be aware of this proposal's threat to our society and to our "guaranteed" Charter right to freedom of speech.

This proposed legislation is not acceptable to us and should not be acceptable to your government.

Sincerely,

s.19(1)

**Karin Brothers** 

copy to The Hon. Minister of Canadian Heritage <u>Steven.Guilbeault@parl.gc.ca</u> <<u>Steven.Guilbeault@parl.gc.ca</u>>

From:	Kate Chapman
To:	ICN / DCI (PCH); MP Steven Gullbeault; justin.trudeau@parl.gc.ca
Cc:	Info@rebelnews.com
Subject:	Digital Citizen Initiative - NO to Censorship
Date:	August 10, 2021 11:55:56 AM

# Canadians are AGAINST censorship of the internet, AGAINST monitoring and censorship of social media, and AGAINST censorship of free speech. We will not allow C-10, C-36 or any similar legislation to pass.

We say NO. You do not own the internet. You do not own Canadians, or tell us how to act, what to think, or with whom to associate. You are not our Masters, Rulers, Owners, Parents, or Guardians. We did not abrogate our personal responsibility and freedom to you when you were elected. As a Canadian Citizen, over the past 15 months, I have watched with horror our country become a fascist police state run by ruthless, cruel, corrupt, anti-human health overlords. So-called "doctors" who have violated their oaths and every single item in the Canadian Medical Association Code of Ethics and Professionalism. Politicians and governments who are completely out of touch with the People and who seem to think it is their right to treat Canadians as brainless idiots incapable of running their own lives, and that the entrenched and sacred Rights and Freedoms so precious and integral to Canadian identity can be disregarded at the whim of unelected and unaccountable autocrats.

We say NO. May I remind you?

- · Governments exist to serve the People. It is NOT the other way around.
- The Health System exists to serve the People. It is NOT the other way around.
- . The Police exist to serve the People. It is NOT the other way around.
- . The Senate exists to serve the People. It is NOT the other way around.

Every single action, every single policy from this current government has been about power and control, not about Health, not about Safety, not about the public interest. Bills C-10, C-36 and any other censorship bills are a gross and unacceptable assault on Canadian free speech and the right to individual autonomy. This "daddy knows best" attitude of governments about their roles in the lives of the People is despicable and completely contrary to the precious and universal right to Free Speech, without government censorship.

It is outrageous and hypocritical that current governments in Canada themselves "incite hate, promote violence and extremism [and] other illegal activity" (direct quote from your "Have your Say" website) in our country while self-righteously condemning ordinary Canadians for expressing their opinions or attempting to have reasonable debates about issues. Churches were not being burned with impunity <u>before</u> the release of government records and so-called media releases regarding cemeteries at former residential schools (which were conceived, set up, and run by the Canadian government). FIFTY churches burned. The government is directly responsible for the harm caused to indigenous Canadians through these schools and is directly responsible for causing the recent burning of churches, yet seeks to silence ordinary Canadian voices who speak out or dissent or disagree with them or merely try to provide and discuss facts. The current government condemns what it loftily decides to be "hate" speech as potentially causing "harm" or inciting people to violence and hatred, while it itself has directly incited (encouraged) people to despicable violence of burning sacred buildings and appears to condone the violence, both tacitly and openly, while crying crocodile tears on camera.

I am not a drone in a hive. I am not seven-of-nine in a Collective. We are not "all in this together." I am an individual with individual Rights and Freedoms that are guaranteed by the Canadian Charter of Rights and Freedoms. I say "NO" to the continued madness from corrupt, anti-human

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

governments whose agendas of complete domination and control of every aspect of Canadian life Action is frighteningly and disturbingly clear.

Canadians are AGAINST censorship of the internet, AGAINST monitoring and censorship of social media, and AGAINST censorship of free speech. We will not allow C-10, C-36 or any similar legislation to pass.

K Chapman Canadian Citizen

From:	sachatdrury
To:	ICN / DCI (PCH)
Subject:	Strongly oppose
Date:	August 9, 2021 3:16:52 PM

Hi,

I strongly oppose the government creating a new framework to regulate social media and online content.

This is a very slippery slope and we're already seeing an unprecedented amount of censorship. We do not want more.

The RCMP can deal with online hate speech, terrorism, and child exploitation - this is NOT the role of government.

Sacha Elliott-Drury, ND

s.19(1)

Sent from my Bell Samsung device over Canada's largest network.

From:	Elena O. Pezzutto
To:	ICN / DCI (PCH)
Subject:	Bill C36 is Ultra Vires
Date:	August 8, 2021 9:54:26 PM

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St Gatineau QC K1A 0S5

RE: Have your say: The Government's proposed approach to address harmful content online

To Whom It May Concern:

I am writing about the internet bill, C-36, a bill that will amend the Canadian Human Rights Act, the Canadian Human Rights Commission and the Canadian Human Rights Tribunal to adjudicate "hate speech" and complaints. Firstly, all of these proposed amendments are ultra vires, especially if they seek to put constraints on women's sex-based rights in favour of gender ideology and trans rights. Governments and politicians simply do not have the authority to pass such laws.

If you do pass these laws - such as Bill C-16, which amended the Canadian Human Rights Act to add gender identity and gender expression to the list of prohibited grounds of discrimination - you are simply passing laws that are already void, and which one day will be repealed as the court cases sure to come reach the SCC. Gender identity is NOT a Charter protected class, which you know. You are simply attempting to circumvent that fact.

So, you have *already* crossed the line attempting to replace sex with gender identity. This violates women's Constitutionally-protected civil liberties and our Charter-protected sex-based rights.

Now you want to attempt to censor our speech online and prevent us from voicing our disagreement with these violations of our sex-based rights and our civil liberties -- which you do, for example, when you house trans-identified males in female prisons, a cruel and unusual punishment if ever there was one, since it subjects female inmates to sexual assault, pregnancy, and other forms of violence. Please bear in mind that at least 70-75% of all TiMs are heterosexual, and NOT homosexuals. They are a threat to women. (See Blanchard, for example.)

Please repeal all of these laws, and please stop attempting to pass more of them. They are ALL ultra vires, as the Department of Justice has no doubt already informed you. Women won't tolerate it. You must understand this fundamental fact: We did not spend our lives fighting for our rights, only to have a new iteration of male misogyny override them.

Sincerely, Elena O. Pezzutto

Sent from Mail for Windows 10

From:	Δ.	The Access to Information
To:	ICN / DCI (PCH)	
Subject:	Discussion regarding PROTECTION OF PRIVACY AND REPU	TATION ON PLATFORMS SUCH AS PORNHUB
Date:	August 8, 2021 5:09:48 PM	

Hello,

s.19(1)

am

I am sharing my perspective as I

sensitive to the need to combat abuse online, especially with regards to sexual content, but I also believe that this can be done without harming sex workers in the process.

On the other hand, regulations can put us in harms way if not written with care. For example, if there were a rule for any website hosting adult content to have a 24hr response time,

Regulations need to account for smaller businesses and not further monopolies, especially in one of the only industries predominantly lead by women, LGBTQ2S individuals, and disabled people. There are ways to write regulations that both prevents non-consensual content from remaining online and also does not destroy the businesses of thousands of women.

I do caution against discouraging attempts at moderation by being overly strict. American law has demonstrated that legal liability for uploaded content can make platforms wash their hands of moderation which enables harmful content to proliferate unchecked in the shadows. It's much better for content to be in the open where it can be checked, and also better for moderators to catch much of the bad content than none at all, because nobody can ever catch all of it. It would also do harm to push public social media sites like Twitter or Reddit to ban all adult content entirely rather than face regulations that are overly onerous and that carry heavy liability. Being able to both advertise and network in public prevents a lot of exploitation and allows for adult performers and

Document communique en vertu de la Loi sur l'accès à l'information. Document released pursuant to

models to share safety information and negative experiences. A lot of the merits of decriminalized communication for sex workers was covered during the Bedford case of 2013, and digital sex workers benefit just as much as in-person sex workers do.

Additionally, a useful standard in the US adult industry is the use of what are called "2257 forms" which are essentially model releases indicating a person is 18+ and consent to the distribution of the material filmed that day, and are kept either available by request by the authorities or uploaded to the video service website as well. This is a standard in line with non-adult model releases, and given how many performers in Canada also distribute through the US it would cause next to no disruption to the industry while still providing proof of consent and age for sexually explicit materials.

I'm very concerned by the inclusion of language around content where "it is not possible to assess if consent to the distribution was given" by looking at it. It may seem upon writing this that the meaning is clear, and I'm reasonably certain I know the kind of images intended to be captured by this language, care should be taken not to stifle free expression by being overly broad. Depending on who is interpreting, this could be as narrow as public upskirt photos, **s.19(1)** 

or as broad as any amateur video or fictional BDSM content. Some ideologues believe that no woman could consent to any pornographic content, which is blatantly false on the face of it given the numerous sex workers who affirm otherwise.

Lastly, the prominence given to a religious lobbyist from another country and the neglect shown to Canadian sex workers who would be directly affected by any regulation into sexual content online is beyond unacceptable to me. Those most effected by proposed legislation or regulation should be the most important voices to listen to. Also given that all of the problems associated with PornHub and the adult industry are magnitudes larger on mainstream social media, this sort of specifically directed regulation is irresponsible and will not adequately address non-consensual sexual content online. Any website with user-uploaded content has the potential for harmful usage, whether sexual content is the primary focus or not. The facts are that Facebook contributes more to sexual exploitation of children than PornHub does, so any regulations aimed at preventing such on PornHub should not ignore the impact of Facebook and other similar social media companies.

Thank-you for your time, and I hope that you take the potential impact these regulations could have on the businesses of women, LGBTQ2S, and disabled people into account.

Azura Rose

Land Allen
ICN / DCI (PCH)
Free Speech
August 8, 2021 3:20:48 PM

August 8, 2021

### то

the Canadian Government Ottawa

### FROM

Andre Houle

s.19(1)

#### SUBJECT: Attack on FREEDOM OF SPEECH

Trudeau and Guilbeault have created a very large speech censorship plan for the internet applicable to Facebook, Twitter, You Tube, Instagram, etc., which has developed into a plan that surreptitiously will also silence anyone that dares to insult politicians or make political commentary that does not please the Liberals and or the Prime Minister. They themselves, have silenced Parliament participation by doing their business when Parliament is shutdown. What they are doing is shutting down our freedom of speech which is a right that all Canadians have always had. But Trudeau does not like criticisms and he is behaving as if Canada has now cancelled democracy and introduced a Communist regime run by a Dictator.

Shutting down our right to Freedom of speech could be considered a Criminal Offence by many Canadians that will not accept that Dictatorship ruling and will probably end up reacting by an uncontrollable Civil strife that could end up as an uncontrollable civil war that could last for quite sometime. Humans all over the world must have the right of free speech or else. Canadians are going to fight for their right to Freedom of Speech.

From:	Hearth Moon Rising
To:	ICN / DCI (PCH)
Subject:	Government's Proposed Approach to Address Harmful Content Online
Date:	August 8, 2021 12:30:45 PM

Dear Sirs and Other Genders,

I have read the Discussion Page entitled "Government's Proposed Approach to Address Harmful Content Online" and recognize this proposal as dangerous and potentially abusive.

Although I live in the United States, I rely on Canadian feminist media resources such as Vancouverbased Feminist Current for information about women's issues, particularly related to third world and indigenous women. Feminist Current, which is supported by donations, is routinely attacked, both in print and through cyber crime, for frank discussion about women's issues. Discussing sex-based issues—or even claiming that sex exists—is considered "hate speech" by many transgender activists such as Morgane Oger. At the very least, online "hate speech" laws will chill feminist discussion and divert resources into fighting accusations. In cancel culture strategy, "the process is the punishment," meaning that the diversion of time and energy to fighting complaints and attacks bleeds organizations and individuals of time and money even when complaints are unsubstantiated. The Canadian government is proposing changes to make the process even more onerous.

I have followed the debacle of Jessica Simpson nee Yaniv's "human rights" complaints regarding female salon workers refusing to handle testicles. These complaints, ultimately dismissed, were traumatic for the women involved. I am aware of how the complaints process in Canada has thoroughly been hijacked as a form of abuse. Those most affected are poor and indigenous women.

Sincerely, Hearth M. Rising



Virus-free. www.avg.com

From:	Jocelyne M. Beaulne
To:	ICN / DCI (PCH)
Subject:	Avis sur l'encadrement des réseaux sociaux
Date:	August 8, 2021 12:11:43 PM

### Bonjour !

J'estime que nos lois s'occupent déjà suffisamment des cinq points soulignés par ce nouveau projet de loi que j'estime par conséquent inutile.

Avec la création de nouveaux organismes, dont une sorte de tribunal en ligne, j'estime que le Canada s'apprête à un retour vers la censure et éventuellement vers un totalitarisme numérique puisqu'on prévoit un éventuel lien avec la GRC et le SCRS sans parler des amendes possibles pour les plateformes.

Il y aura toujours de l'arbitraire, surtout quand il s'agira d'interpréter ce qui se rapporte à un sentiment comme la haine. Je me demande bien avec quel thermomètre les différentes plateformes concernées pourront mesurer ces nuances très subtiles.

Je pense que c'est absolument contraire à ce qu'est une démocratie libérale qui protège les libertés individuelles, démocratie libérale dans laquelle nous somme censés vivre.

Par contre, je conçois que toutes ces mesures et comités donneront prioritairement de l'emploi à ceux qui sont près du PLC, encore une fois.

Respectueusement,

Jocelyne M. Beaulne



Garanti sans virus. www.avast.com

 From:
 Michel Monier

 To:
 ICN / DCI (PCH)

 Subject:
 Contenu préjudiciable en ligne.

 Date:
 August 8, 2021 10:50:48 AM

Le gouvernement n'a pas à s'immiscer dans le contenu en ligne.

MICHEL monier

Envoyé de mon iPad

From:	Anthony Rader
To:	ICN / DCI (PCH)
Subject:	censorship of the internet
Date:	August 7, 2021 4:31:34 PM

#### To Whom It May Concern,

I am writing you to voice my lack of support and concern over your government's intention to censor the internet. There is no reason to do so that I can see. Laws already exist to protect Canadians from harm. Frankly, along with paying the media this appears to be no more than another attempt by your government to eliminate criticism. Freedom depends on information, all information, whether we find it insulting or not. It requires people to be thick skinned as they may not like what they are hearing. That includes the current Liberal government. If you claim to be for freedom and democracy, then you MUST support that claim by allowing freedom of information rather than censorship, even if that information is harmful to your government. Historically there were a number of people who controlled what the media could or could not say. Here's a few names: Hitler, Mussolini, Castro, Lenin and Chairman Mao. They all were members of political parties. Let me put this another way. Is your loyalty to the Liberal Party and holding power or is it to Canada and the freedom of its people? This bill doesn't speak to the latter. I urge you to withdraw it.

Anthony Rader

s.19(1)

From:	Justin Campbell
To:	ICN / DCI (PCH)
Subject:	Online Security
Date:	August 7, 2021 1:58:03 PM

Hello to whomever this may concern. I am writing this to express my opinion towards bills such as bill C-10 and other of similar types. I personally believe that people should be allowed to choose what they say think and see themselves, we are told these bill are being put into place for reasons such as cracking down on illegal content. The 'illegal' content being pursued is already illegal and can be followed up on according to law without the help of new bills being implemented. These bills only create censorship for things outside of the illegal scope and make things that would be legal in any other aspect illegal according to bills like these. How it appears is that you are creating more guidelines to make what would be legal in any normal sense suddenly illegal according to the guidelines created in bills like these. In this process it only further censors the every day Canadian citizens. Targeting things such as child pornography is something important that must be done but there is a fine line you are towing, such as imposing on citizens personal private rights. As far as I know to keep an eye on such troubling behavior all we would need to do is talk to the RCMP, from there get them to create an internet surveillance team for this specific thing, or others. That way you are not including things that are not actually related with the issue, or unfairly censoring something that could be construed incorrectly out of context. The government may have the responsibility to look out for its citizens but not to take away their individual thoughts, feelings and expressions.

Another point I would like to touch on is the fact that people not being able to express their personal opinion about a politician and having it possible being labeled as "hatred" (as defined in section 319 of the criminal code) is dangerous, there are times where politicians need to hear how people are unhappy with them be it criticism or not fully speaking for the rights of the people. Some may take it to far but those are the outliers. When becoming a politician someone becomes a public figure, being a public figure means that you work for the public and should be seen and assessed by the public. Any politician is being paid by the public by means of publics taxes, they work for the people and should expect feedback from the people. When being told that it will only effect how people can refer to politicians on mainstream media I think that in itself is an issue, is a private person posting an opinion on the internet and tagging a politician to show how they are unhappy with things because trying to reach out to a local official has had no results? Does that make it harassment or bullying? Yes, I admit that threats and harm coming to a person are not ok but censoring all feedback is a dangerous slope. The bar for what is even considered "mainstream" is not set very high and with an evergrowing population having something like one million followers becomes smaller and smaller due to populace proportions.

These are merely my own personal concerns going forward on internet security law and I would like to thank you for taking the time to read this and hope you have a god day.

-Justin Campbell

From:	Robin Alexander The Access to Infor	n
To:	ICN / DCI (PCH)	
Cc:	Anna Sainsbury	
Subject:	GeoComply Response: Government of Canada Harmful Online Content Consultation	
Date:	August 5, 2021 5:01:13 PM	
Attachments:	Government of Canada Harmful Online Content Consultation GeoComply Response 8 2021.pdf	

To Whom It May Concern,

Please find attached GeoComply's response to the Government of Canada's Harmful Online Content Consultation.

Thank you and please let me know if there is any additional information I can provide which may be of interest.

Sincerely,

**Robin Alexander** 

Robin Alexander Senior Regulatory Affairs Specialist robin@geocomply.com | geocomply.com

GEOCOMPLY Geolocation You Can Bet On linkedin | twitter

CONFIDENTIALITY NOTICE: The information contained in this email message is intended only for use of the intended recipient. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please immediately delete it from your system and notify the sender by replying to this email.

# GEOCOMPLY

DocuSign Envelope ID: 9A8E5AD4-1CEA-4E8B-8EDF-7AD6087CA4BF la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act

8/5/2021

**Digital Citizen Initiative** Department of Canadian Heritage 25 Eddy St Gatineau QC K1A OS5 Via email: pch.icn-dci.pch@canada.ca

To Whom It May Concern,

### RE: GeoComply Response to the Canadian Government's Proposed Approach to Address Harmful Content Online

On behalf of GeoComply Solutions, thank you for the opportunity to engage with the Canadian Government, to discuss the proposed approach to address harmful content online and the important matter of the use of technology in relation to child sexual exploitation and abuse (CSEA) content.

GeoComply is committed to leveraging our technology and insights to propel social responsibility initiatives, including the protection of vulnerable people online.

By way of this letter, GeoComply addresses the tools and technologies that are exploited by illicit online actors to share, upload and distribute harmful online content, including CSEA content. Our feedback is based on our experience operating globally in the geolocation and identity space, and focuses on technology necessary to better protect persons online. It is our hope that by informing you of the advanced tools and technologies available to mitigate against the distribution of illicit content and fraud, we can collectively make the internet a safer place for all consumers.

GeoComply provides fraud prevention and cybersecurity solutions that detect location fraud and help verify a user's true digital identity. Our award-winning products are based on the technologies developed for the highly regulated and

GeoComply.com solutions@GeoComply.com +1604.336.0877

## DocuSign Envelope ID: 9A8E5AD4-1CEA-4E8B-8EDF-7AD6087CA4BF GEOCOMPLY la Loi sur l'accès à l'information Document released pursuant to

complex U.S. internet gaming (iGaming) and sports betting market. Beyond iGaming GeoComply provides geolocation fraud detection solutions worldwide, for streaming video broadcasters and the online banking, payments and cryptocurrency industries.

### **Technology Contributing To Child Sexual Abuse:**

Child sexual abuse online is unfortunately enabled by the ability to anonymously share data on the internet. Many online platforms currently do not collect the data within their age and identity protocols that are necessary to protect children online. As a result, criminals are able to distribute and circulate CSEA material under false or obstructed identities, evading oversight. For example, A <u>BBC investigation</u> found ineffectual age and identity systems for the OnlyFans platform, causing the circulation of child pornography.

Moreover, the data that has traditionally been collected as part of age and identity protocols can often be manipulated or spoofed. For example, Facebook's 2020 Securities and Exchange Commission (SEC) <u>10-K</u> filing states the following:

"Our data regarding the geographic location of our users is estimated based on a number of factors, such as the user's IP address and self-disclosed location. These factors may not always accurately reflect the user's actual location. For example, a user may appear to be accessing Facebook from the location of the proxy server that the user connects to rather than from the user's actual location."

Similarly, Twitter's SEC 2020 10-K filing states the following:

"In addition, geographic location data collected for purposes of reporting the geographic location of our mDAU is based on the IP address or phone number associated with the account when an account is initially registered on Twitter. The IP address or phone number may not always accurately reflect a person's actual location at the time they engaged with our platform. For example, someone accessing Twitter from the location of the proxy server that the person connects to rather than from the person's actual location."

GeoComply.com solutions@GeoComply.com +1604.336.0877

# GEOCOMPLY

la Loi sur l'accès à l'information Document released pursuant to the Access to Information Act

However, IP addresses are one of the easiest and cheapest data points to spoof, with <u>1 in 3 internet users using a VPN</u>. One of the first layers of protection a bad actor will utilize to mask their true identity is a tool to spoof their location, such as a proxy service, virtual private network (VPN), Tor, or other type of anonymizer.

The ability of unverified, unidentified users to upload and share illicit content online was highlighted by recent <u>allegations</u> made against PornHub (owned by MindGeek). Accused of hosting of CSEA and non-consensual content, MindGeek made the following <u>statement</u> before the Canadian Ethics Committee:

'MindGeek preserves data related to all identified and reported CSAM incidents to permit law enforcement investigation. This includes the content itself, the user's details, and, where available, the IP addresses associated with the user's access to our platforms.'

Unfortunately, a method to spoof an IP address is usually the first tool in a bad actor's arsenal before conducting some nefarious activity online, including the sharing of CSEA material or other illicit content.

### Technology To Fight Against Child Sexual Abuse:

To help protect children online, mitigate illicit activity and uncover anonymous actors, we suggest utilizing geolocation data and spoofing detection within identity verification processes on platforms where this activity may occur. Advanced geolocation and location fraud detection capabilities can instill greater trust and integrity in online transactions.

GeoComply's geolocation and spoofing detection technology has successfully been deployed to address this use case, with the Child Rescue Coalition (CRC).

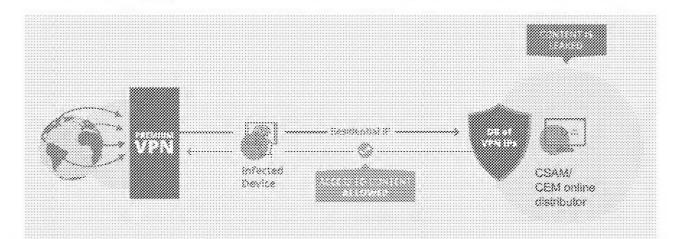
GeoComply's partnership with the CRC began through the donation of our solution, GeoGuard, to the non-profit organization. GeoGuard provides multi-layered fraud

GeoComply.com solutions@GeoComply.com +1604.336.0877

# GEOCOMPLY la Loi sur l'accès à l'information. Document released pursuant to

protection against VPNs, proxies, peer-to-peer networks, and other types of data manipulation, which the CRC utilizes in their analysis of the data relating to CSEA material, to provide actionable intelligence to law enforcement.

The value in GeoComply's technology in providing advanced intelligence to law enforcement, relating to the distribution and sharing of illicit content online, has been exemplified in a recent investigation conducted by the CRC and relevant law enforcement agencies. GeoGuard provided enhanced insights relating to the anonymizers an offender leveraged when engaging with and distributing CSEA material. With GeoComply's technology, the CRC were able to identify that the offender exploited residential proxy services to attempt to mask their illicit online



activity (see the below diagram).

To protect persons online, the following recommendations can be made:

- Utilizing geolocation data and proxy/spoofing detection to combat trafficking and protect children;
- Enhancement to location data in suspicious activity reporting:
- Identifying location based typologies relating to online criminal behaviour.

GeoComply.com solutions@GeoComply.com +16043380877

# GEOCOMPLY

Docusign Envelope ID: 948E5AD4-1CEA-4E88-8EDF-7AD5087CA48FOCUMENT COMMUNIQUÉ EN VERTU de la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act.

### Final Remarks

GeoComply offers these comments to assist the Canadian Government in its mission to safeguard persons online. Thank you for your commitment to preventing online harms and we welcome the opportunity to discuss these matters in further detail at your next convenience.

Yours sincerely,

-DocuSigned by:

anna Sainsbury ~0A7DD640E74D447 ... Anna Sainsbury

Co-Founder and Chairman Anna@geocomply.com

1750-999 West Hastings Street Vancouver, SC V8C 2W2

GeoComplycom solutions@GeoComply.com +16043380877

Docusion Envelope ID: 9ASESAD4-1CEA-4E88-3EDF-7AD5037CA48FOCUMENT COMMUNIQUÉ EN VERTU de



la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act.

1750-999 West Hastings Street Vancouver, SC V6C 2W2 GeoComply com solutions@GeoComply com +16043380877

From:	Anjel Grace
To:	ICN / DCI (PCH)
Subject:	Adult content stakeholder
Date:	August 5, 2021 2:37:12 PM

### Hello,

I really hope the Canadian government is not thinking about making it even harder to live in this world by making it even harder for people to make money any way they see fit. Sex is not bad. Nudity is not bad. Stop the stigma.

Many people with disabilities, chronic illnesses, mental health issues, and other things that prevent them from being able to hold steady jobs or gain enough income from other types of employment use sex work to make money to put food on the table for themselves and oftentimes their children. Making it harder to promote sex work online puts these people at risk of starvation or taking to the streets where the likelihood that they will be murdered increases.

Furthermore, the cost of living everywhere continues to rise, while pay for most jobs does not. Sex work is increasingly being turned to because of this increasing wage gap. During a pandemic, as we are in now, online sex work has also allowed people to stay safe at home while making money from sex work or from buying experiences from sex workers instead of going out and hooking up and potentially spreading COVID.

There are many consensual sex workers. Increasingly, social media is a necessary means of reaching audiences online. Restricting swx workers from social media platforms would be devastating to many.

From:	Kate Sloan
To:	ICN / DCI (PCH)
Subject:	Free speech regulations
Date:	August 5, 2021 12:39:45 PM

### Hello,

I am writing to strongly oppose "the government's proposed approach to address harmful content online."

As we've already seen with laws such as <u>SESTA/FOSTA in the U.S.</u>, attempts to control "harmful content online" always impact sex workers in the strongest and most negative ways of anyone affected. Countless sex workers have lost their livelihoods and even their lives as a result of these laws, since they are no longer able to advertise on trusted websites, vet their clients appropriately, or even build an audience on many social networking platforms.

More broadly speaking, any attempt to censor the internet is worrisome because the internet is one of the few places where true free speech is possible these days, especially for marginalized populations such as sex workers, Black people, and queer and trans people.

Please oppose this terrible idea if you care about the free internet and the continued safety of sex workers. I certainly do.

Kate Sloan (she/her) Journalist, blogger, author Cohost, The Dildorks & Question Box Twitter | Instagram

From:	Anita Bedo
To:	ICN / DCI (PCH)
Subject:	Harmful content online
Date:	August 4, 2021 10:52:38 PM

#### Good day,

My comment is that UNDER NO CIRCUMSTANCES, should ANY DISCUSSION, POST, MEME, VIDEO, AUDIO, REPORT, OR ANY OTHER EXPRESSION regarding COVID be censored. There should be open and transparent exchange of information, views, perspectives, findings, judgments, debates, criticisms, or opinions regarding the virus itself, the injections, masking, lockdowns, sanitizing, research, testimonials, deaths, injuries, testing, reporting, record keeping, diagnosis, symptoms, government mandates, legislation, public health orders, corruption, racketeering, collusion, finances, the World Economic Forum, the World Health Organization, the World Bank, the Chinese Communist Party, the US election, ANYTHING AND EVERYTHING even remotely related to this 'pandemic'. This sets a very dangerous precedent for the future 'pandemics' that we know are going to materialize if we let them.

I have never seen such rampant censorship in social media, mainstream media, within government, etc. It's horrifying and disturbing. There is no excuse - no 'hurtful' comments can justify the destruction of free speech, particularly when lives are at stake. My current main concern is the destruction of free speech on COVID. The biggest danger is confining all discussion to the approved fraudulent narrative. I do not consent.

Thank you, Anita Bedo

s.19(1)

### Bonjour,

Voici mes commentaires par rapport à votre projet de loi voulant encadrer les discours haineux.

Le projet de loi veut encadrer :

- Les discours haineux
- L'incitation à la violence
- Le terrorisme
- · L'exploitation sexuelle des enfants
- Le partage de photos intimes sans consentement

Ce sont toutes des actions illégales déjà encadrées par la loi. Les réseaux sociaux sont déjà extrêmement censurés. Par ailleurs, les réseaux sociaux exercent déjà de la censure très large sur des commentaires qui ne sont pas concernés par la loi.

Vous essayez de faire passer le contrôle des discours en agglomérant l'exploitation sexuelle des enfants et le partage des photos intimes sans consentement. Qui est pour l'exploitation sexuelle des enfants et le partage des photos intimes sans consentements? Personne. Cette pratique est très insidieuse et mesquine.

Vous voulez également bloquer les plateformes (Facebook, Twitter, Youtube, Gab et Tiktok) au complet si elles n'agissent pas en 24 heures. Je perçois une odeur totalitaire du type communiste chinois dans votre projet.

D'ailleurs, vous devriez renommer la Commission de la sécurité numérique du Canada pour le Commission de la censure du Canada.

Votre agenda est tellement extrême que le Canada serait le premier pays à disposer d'un tel mécanisme. Vous voulez avoir un contrôle total sur les débats et par conséquent imposer votre idéologie en prenant les citoyens pour des êtres si fragiles et immatures que le gouvernement doit les couvrir comme des œufs.

Vous pensez vouloir protéger les citoyens, mais vous représentez le pire régime qui existe avec votre idéologie marxiste. Soyez assuré que si vous déposez cette loi, la population se mobilisera pour vous retirer du pouvoir et détruire cette loi.

 From:
 Elias Everett

 To:
 ICN / DCI (PCH)

 Subject:
 Online Regulation (legislative and regulatory framework)

 Date:
 August 4, 2021 3:25:53 AM

I've read a few articles, and as a Canadian and stakeholder I can easily say this proposal does not hold the interests of me, nor anybody I have ever met, at heart. I hope this proposal can be thrown out in favor of actually respecting the privacy and work of Canada's citizens.

The phrasing is vapid and vague, which on its own should be enough to throw it out.

If something needs to be done, this isn't what to do.

Thank you for your time.

From:	Justin De Marco	
To:	ICN / DCI (PCH)	
Subject:	Comments regarding: Proposed approach to address harmful content online	
Date:	August 4, 2021 3:25:36 AM	

### Hello,

I am writing regarding the government's proposed approach to regulating hate speech online. I am <u>deeply disturbed</u> by the move to regulate and criminalize free communication between individuals online. While I generally support efforts to address (1) terrorist content, (2) nonconsensual sharing of intimate images and (3) child sexual exploitation content, the provisions around "hate speech" and "content that incites violence" are dangerously broad and frankly ungovernable. I am opposed to these clauses in the legislation for several reasons.

### Our current laws are perfectly capable of addressing these issues already

As listed in the discussion guide, the Canadian Criminal Code already contains provisions against inciting hatred against identifiable groups. Canadian courts have adjudicated this issue many times. Likewise, those targeted by hate speech have legal remedies in the form of civil lawsuits for libel or slander. We do not need to create more burdensome tools along with an agency that is responsible for policing content online. Its mere existence will incentivize its employees to find and "address" the various complaints brought before them in a way that is bound to expand the definitions of hate speech and restrict free communication online. It will create institutional bloat in government and ultimately create more problems than it solves.

### It will have a chilling effect on free speech

Given the possibility of steep penalties against social media platforms, these companies are bound to over-react in relation to any complaint, lest they be penalized by the government for failing to do so. This will inevitably result in an over-policing of online communication and a tendency to take down any sort of content that might be deemed "hateful" by an offended party. Whether it actually is hateful or isn't does not matter because online platforms will always err on the side of caution and take down content on the off-chance it is indeed hateful speech. Indeed, there will be little marginal benefit to online platforms allowing any sort of controversial content to remain while there will be a massive cost to allowing it to remain. As such we can expect the platforms to consistently take down anything that might remotely be construed as hateful, nuances be damned. This sort of asymmetric response will have a dangerous effect on the free exchange of ideas, especially as it relates to any kind of sensitive topic that impacts a protected group.

I can think of many recent examples of public discussion that has been described by the most vocal and extreme advocates as being hateful.

- Is discussion around the difference in athletic performance between natural-born women and trans women transphobic? Many advocates seem to think so. Yet there are undeniable facts of biology that are necessary to discuss around this issue if one wants to enact policies that are both fair to the athletes and respectful of everyone's human rights. Some seem to think that any sort of discussion that recognizes differences in performance is necessarily transphobic.
- Can one be opposed to racism while also being opposed to the pedagogical tenets of "anti-racism" and "critical race theory"? I certainly believe so. Yet if one were to listen

Document communique en vertu de la Loi sur l'accès à l'information. Document released pursuant to

to the advocates of these policies, any opposition to them is racist (never mind that a from Actinuation huge majority of minorities oppose these practices). Under these new laws such opposition might be construed as hate speech.

Over the last several years, activists have shifted the boundaries and the meaning of hate speech. Words are now "violence" and merely discussing aspects of reality that stand in opposition to ideological doctrine has been described as hateful. In the United States, The American Booksellers Association recently apologized for "a serious, violent incident" that required "concrete steps to address the harm we caused." Their crime? Including a book that explores the exponential increase in the number of transgender youth in recent years. (LINK) Meanwhile, the Canadian Federation of Library Associations released a statement supporting the principles of intellectual freedom in Canada following the demands of activists for libraries across Canada to drop the same book.

If the provisions surrounding hate speech are included in this law, it will give additional power to activists who seek to shut down discourse. It is crucial that we do not allow this to happen so that we can protect the free communication of ideas.

#### It Will Lead to the Criminalization of Non-Criminal Activity

By creating overly broad definitions of hate speech and creating new tools to combat it, thousands of Canadians will see their lives ruined by being criminalized for non-criminal activity. As we mentioned earlier, true hate speech is already a crime in Canada. But by broadening the law, any Canadian who is accused of hate speech for comments made online and tried by an unsympathetic court could be criminalized for what is essentially a thought crime.

The UK has had more aggressive policing of speech than Canada for a number of years. In that country, "between 2014 and 2019, almost 120,000 'non-crime hate incidents' were recorded by police forces in England and Wales." (Andrew Doyle, Free Speech and Why It Matters) These incidents stay on the accused's records and make it extremely difficult for them to be employable. The mere accusation itself is often enough to sink someone's career prospects, whether it is true or not. In 2018, a 19 year-old was convicted of a hate crime in England for sharing the lyrics of a rap song on her instagram page. She was fined and put under house curfew with an ankle monitor. (LINK) Is this really the kind of country we want to live in? Is this unsavory, even offensive behaviour? Sure. But is it criminal? Certainly not. Yet the proposed legislation would criminalize such offenses and create a class of criminals in Canada who are unemployable and have their lives tainted forever.

#### **Defining Hate Speech is Quasi-Impossible**

Defining hate speech is quasi impossible. What is offensive to me may not be offensive to you and vice versa. Yet by criminalizing this sort of behaviour online, we allow the most sensitive and offended in our society to dictate the terms of acceptable speech. I reject that. I do NOT want Canadian laws to be defined by subjectivity. And the idea that hate speech can be neatly defined so that when it occurs is obvious, clear cut and dry is impossible.

#### It Infantilizes the Public and Destroys Trust in Society

Finally, by denying the public the right to critically engage with the information it consumes,

## Document communique en vertu de la Loi sur l'accès à l'information. Document released pursuant to

lawmakers will stultify the minds of their constituents and destroy the trust that is necessary for democracy to function. Indeed, free thinking is at the foundation of any democracy. Anyone who robs another of the right to establish truth for themselves, robs them of their right to think. In doing so, they destroy the bonds of trust that exist between citizens in a free society. When limits to acceptable thought, no matter the intent behind them, are imposed, it is akin to the government saying "we don't trust you to think for yourself on this issue." Offensive language exists online. That is certainly true. But that is an acceptable cost if the destruction of trust in society is the alternative.

We must do everything we can to protect free speech. It is the fundamental principle that makes our democracy possible.

As such, I am vehemently opposed to the hate speech and content that incites violence provisions of the proposed legislation not because I am opposed to those ideas but because the proposed framework is the wrong remedy. We already have social norms and legislation that addresses the problems this proposal purports to solve. As such, any new legislation will ultimately cause more harm than good. Your own proposal even seems to recognize this by limiting the exceptional recourse provisions (120) to "child sexual exploitation content, or terrorist content." This seems to be a very clear admission by the draftees of the proposal that hate speech is not at all a problem at the same level of urgency or harm to society as the two listed in this provision. If even the draftees don't believe in the necessity of acting aggressively against online platforms on these issues, then why should we accept any of the proposals around this issue?

The protection of liberalism and liberal values is an issue of crucial importance to millions of Canadians. This proposal is deeply anti-liberal and I find it shameful that the Liberal party is reneging on the principles that once made it so great.

Please consider removing the proposed clauses around hate speech from the final legislation.

Thank you,

Justin De Marco

From:	G Grenholt
To:	ICN / DCI (PCH)
Subject:	Online Content Regulation
Date:	August 4, 2021 1:48:23 AM

I'm going to get straight to the point with this. I do not support it.

The idea behind the legislation is honest enough, although the language is too vague. This would open the door for blanket censorship of all 'adult' content that Canadians would have access to. It could negatively affect thousands of small time and independent content creators, and do incredible damage to free speech online.

There are always comments, memes, comics, images, and videos that are made with the point of making real commentary on current global and socio-economic issues, simply made palatable by being made into a funny or NSFW (not-safe-for-work) format that helps what is often a positive or important message spread further, faster.

This will wind up doing nothing but harming Canadians, especially when, not if, when a government entity or these international groups pushing for this type of censorship decides it's got enough of a foothold to make it work.

No Canadian wants human-trafficking, or terrorist activities to be able to simply happen, but this will not help to stop it.

It will only help kill the freedom of the internet.

**R** Hynes

Sent from Mail for Windows 10

 From:
 Al Dakota

 To:
 ICN / DCI (PCH)

 Subject:
 Inquiry on new online content regulations.

 Date:
 August 3, 2021 11:20:30 PM

Hello, I am emailing as a stakeholder to provide input on the content of the new regulations presented.

I would like to point at the implications of the allowance of other forms of free speech being limited as a cause for alarm that could arise if any of these regulations are put in place.

While hatespeech and the causing of violence is a major concern, aspects such as pornographic material appears unnecessary in the long run of public safety.

Artistic expression can fall under pornography in some regards. The nature of interpretation under such regulations could lead to wide spread and inappropriate censorship that could be harmful to the free communications between people. Artisric expression alone being limited by any such regulation stands against free speech. Blanket censorship is a very dangerous concept to attempt to employ and for the interest of free, harmless expression, I believe that such a blanket should not be implemented at all. It is a blatant violation of basic rights to express oneself and if such dangerous and wide spread censorship is allowed then it will open the door for even harsher censorship that could be very damaging to the usefulness, accessibility, longevity, and value of the internet as a whole.

 From:
 Chris Hughes
 Media

 To:
 ICN / DCI (PCH)

 Subject:
 The Government's proposed approach to address harmful content online

 Date:
 August 3, 2021 11:04:25 PM

Hi

I have a brief few words on this matter: stop pursuing this. It is foolish, poorly targeted, and rife for abuse and over reach. If you'd like more details on why I recommend you consult with Michael Geist, University of Ottawa professor and the Canada Research Chair in internet law. However, I suspect, based on his comments and track record, that Heritage Minister Guilbeault is uninterested in any feedback or consultation especially if it is from a critic, especially a scholarly expert.

Chris Hughes

Sent from my iPhone

From: To: Subject: Date:

ICN / DCI (PCH) Contenu préjudicialbe August 3, 2021 7:49:07 PM

Je suis totalement contre de nouvelles lois contre les contenus préjudiciables.

s.19(1)

Le problème est de déterminer ce qui est vraiment préjudiciable de ce qui est légitime.

Les partisans de tous les mouvements idéologiques peuvent utiliser ces lois de façons abusive pour faire taire ceux qui les déranges. Ces lois seraient en elles-mêmes très préjudiciables...

**Gilbert** Poulin

 From:
 Ethan Martin

 To:
 ICN / DCI (PCH)

 Subject:
 Thought police

 Date:
 August 3, 2021 7:29:43 PM

A fundamental human right enshrined upon us as Canadian's is the freedom of expression. I for one will never condone limiting someone's ability to express themselves or someone's ability to disagree or agree with someone else's opinions regardless of my feelings about the topic. Shame on you for even thinking this is a good idea. This sounds like something out of Karl Marx's literature. George Orwell wrote a story called 1984 it was not ment as a manifesto for big government.

Regards Ethan

 From:
 Rob Hennessey

 To:
 ICN / DCI (PCH)

 Subject:
 Censorship

 Date:
 August 3, 2021 3:42:12 PM

I support none of this nonsense.

From:	Monica Granadino
To:	ICN / DCI (PCH)
Subject:	new law on censorship
Date:	August 3, 2021 2:29:56 PM

One of the most important tenets of a FREE society is the right to FREE speech/press. Your so called proposal for a bill to censor or ban or control free speech/press is hidden by using the word "harm or harmful" (Not illegal but harm/harmful)... Who will define harm/harmful? there are already laws against promoting pornography, iniciting violence, terrorism etc. Through Trudeau's proposed bill (yes, he is the one behind this) he will in effect decide what "truth" we should read/hear.

# The Government's proposed approach to address harmful content online

This is something expected from a banana republic, from Cuba, Venezuela NOT Canada. Man up and accept criticism which builds a country and a democracy. I REJECT this proposal. There are already legal. mechanisms in place to protect the public against crimes. This proposal wants to "silence" not to protect.

I HAVE THE RIGHT TO READ AND LISTEN TO WHATEVER I WANT... NOT TO WHAT THE GOVERNMENT WANTS ME TO LISTEN OR READ OR THINKS I SHOULD READ OR LISTEN.

The real problem here is: TRUDEAU CANNOT TAKE THE TRUTH ....

Remember: you are my employee. I pay for your salary.

Thank you. M.Granadino

 From:
 Pierre ACHON
 INE ACCE

 To:
 ICN / DCI (PCH)
 ICN

 Subject:
 Commentaire : Encadrement politique des réseaux sociaux/mardi, le 3 août 2021
 Date:

 Date:
 August 3, 2021 1:27:14 PM
 PM

Commentaire : Encadrement politique des réseaux sociaux/mardi, le 3 août 2021

Non à la proposition de donner aux géants du WEB des pouvoirs étatiques pour imposer une censure.

La censure étatique des opinions politiques est une forme de totalitarisme politique. Cela est inacceptable dans une démocratie. Que le gouvernement de J. Trudeau veuille aller dans cette direction est inquiétant. Toutes les personnes qui défendent la liberté d'expression devraient s'y opposer.

Il y a des lois qui défendent la diffamation d'autrui. La liberté d'expression signifie que même des idées stupides peuvent être dites et donner lieu à débat. Les gens sont capables de faire la différence. Avec la censure, on sait quand elle commence mais on ne sait pas où elle s'arrête.

La censure politique ouvre toutes grandes les portes à l'arbitraire et à la suppression de prises de position non populaires. C'est une façon d'imposer la pensée unique. C'est une atteinte à la démocratie. Pierre Achon,

s.19(1)

 From:
 Candice Hall

 To:
 ICN / DCI (PCH)

 Subject:
 Harmful content on social media

 Date:
 August 3, 2021 11:07:01 AM

The government should have NO say in regulating harmful content on social media platforms. This is a slippery slope which leads to potential loss of free speech. It is not the government's job to hinder communication or free speech of the people. Dr Candice Hall

Sent from my iPhone

 From:
 eddy lachapelle

 To:
 ICN / DCI (PCH)

 Subject:
 bill c 10

 Date:
 August 3, 2021 7:35:10 AM

"Aucun pays, à part les régimes oppressifs et les dictatures, n'est allé aussi loin dans l'encadrement des plateformes numériques.

The quote above is from Le Devoir. You have asked what my opinion is on this matter. And i will keep it short. If you are imitating dictatorships, you are probably doing something wrong. Amibigious definitions and vaste powers can only result in tyrnanny. Stop this.

 From:
 Penny Laird

 To:
 ICN / DCI (PCH)

 Cc:
 Karen M.P. Vecchio

 Subject:
 NO thank you to more censorship

 Date:
 August 3, 2021 6:54:53 AM

To whom it may concern:

Thank you for posting this information here at: https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html

However, from a public point of view it seems to lack integrity to put this "information" in place when parliament has been closed for the summer and it cannot come under critical review from the opposition.

I agree with protecting the vulnerable, removing sexually exploitive material, and against inciting violence. It is the power hidden within this I ask you to not to implement. It takes dead aim at ordinary citizens who post anything on Facebook, Twitter, Instagram, YouTube or other social media.

Canadian laws already prohibit terrorism, inciting violence and other real crimes online. These new proposals invent a vague, new concept called "harm" — which Guilbeault has said in interviews includes insulting politicians and other political commentary. He says it's necessary to silence some voices to let other, preferred voices speak. His words sound like an excerpt from the book *Animal Farm*, a critique of Communist rule. It's just an excuse for censorship. All voices, even if disagreeable or nonsensical have the right to voice their opinion - otherwise no one has free speech.

To be plain, I am very much against bill C-36.

Concerned Canadian citizen, Penellope Laird s.19(1)

From:	and the second se
To:	ICN / DCI (PCH)
Subject:	Re censorship bill
Date:	August 3, 2021 6:33:02 AM
Contraction and the second	

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act.

Yes, censorship bill. It has nothing to do with stopping "harmful content" or "hate speech", and everything to do with stopping criticism of government. We already have laws for hate speech, we don't need more because the Liberals are afraid of a little justified criticism. This Bill is absolutely disgusting, and would have been right up Goebbel's alley had the Internet existed. It's very reminiscent of China's censorship of free speech. But what should we expect from an Occupant of the Prime Minister Office who admires China's "basic dictatorship"? Don't even think of passing this Bill. It has no place in a free constitutional democracy.

James Dyck

Sent from my Galaxy

 From:
 Siegfried Volz

 To:
 ICN / DCI (PCH)

 Date:
 August 3, 2021 4:32:30 AM

No censorship period. Our government can't be relied upon for information. Only free flow of information will ensure for s free society.

 From:
 Wollner

 To:
 ICN / DCI (PCH)

 Subject:
 No to censorship of any type

 Date:
 August 2, 2021 9:27:28 PM

Common sense is not common - especially to government officials.

There are laws in place regarding when an actual crime takes place, free societies have no desire for thought police and censorship.

Absolute NO and NEVER to Bill c-36.

Discussion leads to innovation and understanding, censorship and thought policing end up in tyranny and communism.

Sent from my iPhone

From:	Deborah Derose
To:	ICN / DCI (PCH)
Subject:	online harmful content censorship
Date:	August 2, 2021 6:29:01 PM

Regarding the Federal Government's intention to monitor and censor what they believe to be harmful online content.....

At first glance and in the most superficial manner, the intent and proposal of online censorship appears benevolent, however, as in most matters governed by legislation and the courts, all is subject to interpretation. Harmful content, terrorism, inciting violence while conversationally understood, becomes less well-defined in its

application as it is subject to political pressure and influence. Yes, some use of social media can be deemed offensive to some people but not to others. There are laws on the books governing terrorism, pedophilia, sexual exploitation, and incitement to commit violence. What need does the public have of a government determining upon its own interpretations, what a nation can view online?

Our own government and our American brother spare no words of criticism against Cuba, China, North Korea, and other nations where the government determines what is permitted to be seen and/or published. Their own governments will justify the censorship as being "for the overall good of the nation".

How are we, in the self-described free and democratic West, to have any credibility in judging these other oppressive nations for their censorship while we do it at home? Are we to adopt the very process those nations promote?

If the subject matter was determined to be offensive or threatening or harmful by way of democratic consensus, one might make a decent argument for some control of online content but that is a slippery slope towards an Orwellian "1984" dystopia when the government exercises right of interpretation, legislation and prosecution

This is not the Canada I grew up in, and in my advanced years I clearly remember the disdain we had towards the Soviet Union's control and manipulation of government controlled media and the consequences to dissenters of the official narrative..

Dissent towards our own Federal government or its policies, is the right of citizenship in a democracy. We have laws to prosecute those who commit criminal offences, we have investigative agencies for prosecutorial purposes so what would be the purpose of monitoring and censoring online content that wasn't already subject to laws? Totalitarian governments enjoy this type of power and control. Are we becoming similarly governed?

Allow people to express themselves and if it breaks the law, prosecute the offender and if it does not meet any criminal offence criteria, but is simply offensive in someone's opinion, then they have the freedom to not read or engage in that content.

Free speech that is offensive is not a crime. Government censorship of social media is tantamount to totalitarian ideology. Every Canadian, who understands what our troops fought against in WW2 should find government intervention in online content or social media specifically, unconscionable and of the greatest disrespect to the sacrifices of our troops.

We as a nation, give safe harbour to refugees who flee such totalitarianism and yet, hypocritically, we would censor our own citizens??

No, no censorship[. Not as long as we wish to assert we are a free nation.

Deborah Derose

From:	Ugo DeBiasi
To:	ICN / DCI (PCH)
Subject:	Harmful Content online
Date:	August 2, 2021 6:14:41 PM

At first glance and in the most superficial manner, the intent and proposal of online censorship appears benevolent, however, as in most matters governed by legislation and the courts, all is subject to interpretation.

Harmful content, terrorism, inciting violence while conversationally understood, becomes less well-defined in its application as it is subject to political pressure and influence.

Yes, some use of social media can be deemed offensive to some people but not to others. There are laws on teh books governing terrorism, pedophilia, sexual exploitation, and incitement to commit violence. WHat need does the public have of a government determining upon its own interpretations, what a nation can view online?

Our own government and our American brother spare no words of criticism against Cuba, China, North Korea, and other nations where the government determines what is permitted to be seen and/or published. Their own governments will justify the censorship as being "for the overall good of the nation".

How are we, in the self-described free and democratic West, to have any credibility in judging these other oppressive nations for their censorship while we do it at home? Are we to adopt the very process those nations promote?

If the subject matter was determined to be offensive or threatening or harmful by way of democratic consensus, one might make a decent argument for some control of online content but that is a slippery slope towards an Orwellian "1984" dystopia when the government exercises right of interpretation, legislation and prosecution This is not the Canada I grew up in, and in my advanced years I clearly remember the disdain we had towards the Soviet Union's control and manipulation of government controlled media and the consequences to dissenters of the official narrative.

Dissent towards our own Federal government or its policies, is the right of citizenship in a democracy. We have laws to prosecute those who commit criminal offences, we have investigative agencies for prosecutorial purposes so what would be the purpose of monitoring and censoring online content that wasn't already subject to laws?

Totalitarian governments enjoy this type of power and control. Are we becoming similarly governed?

Allow people to express themselves and if it breaks the law, prosecute the offender and if it does not meet any criminal offence criteria, but is simploy offensive in someone's opinion, then they have the freedom to not read or engage in that content.

Free speech that is offensive is not a crime. Government censorship of social media is tantamount to totalitarian ideology. Every Canadian, who understands what our troops fought against in WW2 should find government intervention in online content or social media specifically, unconscionable and of the greatest disrespect to the sacrifices of our troops.

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

We as a nation, give safe harbour to refugees who flee such totalitarianism and yet, ormation Act. hypocritically, we would censor our own citizens??

No, no censorship[. NOt as long as we wish to assert we are a free nation.

From:	Monique Boulanger
To:	ICN / DCI (PCH)
Subject:	Réglementation sur les médias-sociaux
Date:	August 2, 2021 4:43:36 PM

Bonjour M. le Ministre Steven Guilbeault,

J'écris pour vous signifier mon appui quant à la législation proposée au sujet des abus commis par le biais des médias-sociaux.

Je crois moi aussi en la nécessité de soutenir un environnement en ligne sûr, inclusif et ouvert.

Les cinq catégories de contenus préjudiciables : le contenu terroriste, incitant à la violence, le discours haineux, le partage non consensuel d'images intimes, le contenu d'exploitation sexuelle des enfants en ligne n'ont pas leur place dans mes valeurs et celles de beaucoup d'autres Canadiennes et Canadiens. Merci de construire pour nous tous une société plus juste et plus sécuritaire. Je trouve que l'Initiative de citoyenneté numérique est une très bonne idée et une étape nécessaire à franchir, avec la collaboration de tous les intervenant-e-s pour qui ces enjeux sont importants.

Sincèrement,

Monique Boulanger,

s.19(1)

 From:
 Victoria OHara

 To:
 ICN / DCI (PCH)

 Subject:
 No censorship

 Date:
 August 2, 2021 4:36:52 PM

Our freedom of speech it part of the constitution. Canada has always been a free country and now it is looking like a dictatorship. Strong, proud and free Let us remain Victoria OHara

Sent from my iPhone

## Felicia Mazzarello

From: Sent: To: Subject: Duncan McGregor October 5, 2021 3:30 PM ICN / DCI (PCH) Opposition to harmful online content legislation

Hello,

I am a resident of the and am writing to state my opposition to the proposed legislation that would oblige online service providers to actively monitor for harmful content, as described here: https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html

In my opinion, this kind of active monitoring is not feasible, and attempts to implement it will have a chilling effect on online discussions. This is especially true given the large penalties proposed for offences that allow content deemed harmful to stay up; the service providers will be incentivized to remove questionable content instead of attempting to make a reasonable determination.

While I do not want to encourage content of any of the types listed in that discussion page, I also want to make sure that Canadians are not silenced as collateral damage due to an excess of zeal. I believe that the proposed legislation will do this, and hope that it can be studied further before being introduced.

Thanks, Duncan McGregor

s.19(1)

 From:
 ICN / DC1 (PCH)

 Subject:
 mailto:pch.icn-dci.pch@canada.ca

 Date:
 August 2, 2021 4:05:29 PM

s.19(1)

mailto:pch.icn-dci.pch@canada.ca

To whom it may concern

Canada is OUR country and we believe in the Charter of Rights and Freedoms, up to and including FREE SPEECH!! Censorship of free speech in any form is treasonous!!

Do not continue this attack on our liberties or you will see a Canada that will fight back with a fury, the likes of which that has never been witnessed on our soil before!!

Regards We the people Sent from ProtonMail mobile

 From:
 Tvier Vincent

 To:
 ICV/DCL(PCH)

 Subject:
 How we can stop our Sate Sponsored Hate, Stop arming terrorists and End regime change abroad [update]

 Date:
 August 1, 2021 9:04:59 PM

We already have laws for harmful content. What we need is for our government to stay our of our business, and parliament to swear an oath to stop directly and indirectly arming ISIS terrorists, Israel and other terrorist organizations. We don't want Canada becoming like America, who's Stop Arming Terrorists bill failed in congress after gaining only 13 out of 535 congressional supporters.

H.R.608 - Stop Arming Terrorists Act was introduced by Rep. Gabbard, Tulsi [D-HI] on January 23, 2017. The bill doesn't have any crazy strings attached and its original cosponsors are a mix of Republicans and Democrats — highlighting that it transcends party lines.

"For years, our government has been providing both direct and indirect support to these armed militant groups, who are working directly with or under the command of terrorist groups like Al-Qaeda and ISIS, all in their effort and fight to overthrow the Syrian government," Gabbard said in an interview earlier this year.

The only thing this bill does is prohibit the US government from giving money and weapons to people who want to murder Americans and who do murder innocent men, women, and children across the globe. It is quite possibly the simplest and most rational bill ever proposed by Congress. Given its rational and humanitarian nature, one would think that representatives would be lining up to show their support. However, one would be wrong.

After nearly 5 months since its introduction, only 13 of the 535 members of Congress have signed on as co-sponsors. What this lack of support for the bill shows is that the federal government is addicted to funding terror and has no intention of ever stopping it. First we must create and pass our own "Stop Arming Terrorists Act" long before we preach to others what constitutes "harmful content."

"Social media platforms can be abused and used to incite hate, promote violence and extremism or for other illegal activity."

Our own government, media, and military uses online platforms to promote illegal regime change wars, terrorism abroad, and the bombing of entire civilizations to the stone age, such as Libya, as well as the relocation of Al-Qaeda to Canada.

We (the Canadian government) are the terrorists and we need to stop promoting terrorism and regime change in countries like Ukraine and Belarus. We must stop promoting state sponsored hate speech and harmful fake news directed at Russia, China, Iran, Hamas, Hezbollah, and the other leaders of the civilized world. We need to stop helping the illegal Jewish occupation of Palestine, America, and Britain arm and train ISIS terrorists, and we need to do that long before we start preaching to other about what constitutes "harmful content."

We don't need any more government regulations of freedom of expression and information, we need less. That does not mean you have the right to finance terrorism around the globe. State sponsored terrorism and state sponsored regime-change driven hate-speech is our primary concern that needs to be addressed here in Canada and we need to put an end to our role in financing child be-headers around the world immediately.

Thanks for understanding, like I'm sure you give a shit.

Tyler Vincent

s.19(1)

Stop arming Terrorists!



#### Felicia Mazzarello

From: Sent: To: Subject: Kyle Biggy October 22, 2021 2:44 PM ICN / DCI (PCH) Please stop

s.19(1)

I do not agree with media censorship placed on the doctors, nurses and scientists with alternative views to big pharmaceutical companies. The platform for legitimate debates has been undermined. You have forced the people of Canada to be lead by large groups of companies that care more about profit than the well being of the people.

Sent from my iPhone

From:	Jeri Danyleyko
To:	ICN / DCI (PCH)
Subject:	Government proposals on harmful online content
Date:	August 1, 2021 3:39:49 PM

One area that seems to be missing is online stalking through social media which I think belongs in a category all by itself. Another area that seems to be missing is advertising. The people that produce this stuff are very creative and clever and can easily build subliminal advertising that slips through the cracks.

And how do you propose to enforce fines and/or other penalties? These companies are very wealthy and a fine would likely not be much of a deterrent.

And lastly, the algorithms that are presented to users need to be targeted also. Just targeting a post or article would not be sufficient. Inspecting it after the fact would also be insufficient once the damage is done.

I suspect much of this will be watered down once the lobbyists get to work.

Best regards, Jeri

#### Felicia Mazzarello

From: Sent: To: Subject: Ryan Neate October 22, 2021 11:45 AM ICN / DCI (PCH) Response to Online Harms Legislation

s.19(1)

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards,

Ryan Neate

 From:
 m.canu.

 To:
 ICN / DCI (PCH)

 Subject:
 Projet de loi concernant la haîne sur les réseaux sociaux

 Date:
 August 1, 2021 1:19:00 PM

#### Bonjour,

Je suis complètement en accord avec ce projet de loi contre les plate-formes qui génèrent ces commentaire haineux. J'espère que vous ferez en sorte de faire le ménage pour le bien de tous, mais particulièrement pour la jeunesse vulnérable de celle-ci.

Personnellement, je suis sidéré à chaque fois que je lis sur différent sujets, et surtout, surpris de constater, qu'en si peu de temps une tempête de haine peux apparaitre, comme si c'était un plaisir pour quelques-uns (unes) de s'investir dans ce genre de propos.

Cette minorité qui y participe, sont très présent et facile à trouver sur ces réseaux.ils semblent se faire une fierté d'être entendu et lu.

à l'aise avec l'informatique et je me suis brancher sur internet dès le moment ou on pouvait y avoir acces, car j y trouvais quelques chose d'utile.

Maintenant, avec les années, on peux y voir les conséquences d'une société informatisé, sans règlement laissé à elle même.

Oui,il est grand temps de s'en occuper et le faire correctement pour éliminer ces commentaires dangereux.( C'est utopique d'y penser, mais je ne serais pas contre la fermeture de ces réseaux).

Merci.

## Bonjour,

Je suis totalement contre se projet, la liberté de parole doit absolument être libre et sans conséquence. Chaque citoyen est libre de pensé et d'écouté qui il veut.

Sommes-nous au Canada ou **au Chinada**??? La question se pose!!!! Si vous voulez vous attaqué à quelques choses, **attaquez-vous à la "nouvelle pensée** unique"!!!! À **l'absence de tout débat** relié à la pensée unique ou encore à la **violence phycologique** du gouvernement Caquiste!!!

On se fait menacé par le gouvernement de la CAQ, pratiquement chaque jour que Dieu fait, et de façon des plus insidieuses, en êtes-vous conscient au moins!!! Je vous invite à regardé du côté des médias, des "Mario Dumont" qui disent en pleine télévision que si notre frère, notre beau-frère ne pensent pas de tel ou tel façon de coupé les liens, de le barré sur facebook, ne plus le voir!!! Mais ou sommes nous rendu???? Voulez-vous ben me le dire, c'est carrément de l'incitation à la haine dans la famille, c'est extrêmement grave!!!

Regardez les Patrick Lagacé, les Richard Martineau (pour ne nommé que ceuxlà), qui traitent les citoyens d'édenté, de covidio, d'égoïste!!!! Qui paye leurs salaires avec de grosse subvention??? TOUS les citoyens, et non pas juste les citoyens qui pensent comme eux!!! D'ailleurs on devrait réviser les subventions à la baisse avant de faire du délestage dans les hôpitaux!!! Qu'est qui est le plus important, sauvé des vies dans les hôpitaux ou payé des médias pour insulté les gens qui paient leurs salaires!!!

Une société ou règne la pensé unique, est une société qui n'avance plus. C'est une société communiste et non pas une société démocratique!!! Vous devez à TOUT PRIX laissé le choix, le libre arbitre à chaque citoyens qui (n'oublions pas paye vos salaires) par leurs grosses taxes et impôts, la pleine liberté de dire, de pensez, d'écrire se qu'il veut, c'est capital.

# Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

Alors je m'objecte FERMEMENT à votre projet de loi et je vous invite à une fron Act profonde réflexion sur l'importance de la liberté de choix. Vous devriez plutôt regardé du côté de la violence phycologique de notre gouvernement Caquiste et des médias Québécois. Faire un projet de loi pour empêcher une telle violence dans leurs propos. Dois-je vous rappelé que les médias sont là pour rapporté LES FAITS, non pas pour émettre leurs opinions personnel avec de la propagande à la haine.

Aujourd'hui, plus que jamais, on voit le résultat!!! Un peuple divisé ou règle la haine, la chicane, dans des familles, avec les amis. Le peule Québécois à toujours été reconnu pour l'entraide, la solidarité, mais étant victime de la violence phycologique journalière du gouvernement et des médias, je suis forcé de constaté à quel point, ils sont en train de détruire nos plus belles valeurs. C'est GRAVE ET MÊME TRÈS GRAVE!!!!

Alors je vous invite à regardé ou est le véritable problème et de travaillé sur un projet de loi visant à le réglé. La pensée unique va agrandir le problème, les gens réclament des débats qui nous sont déjà interdit et maintenant vous voulez obliger les gens à ne plus s'exprimé, un instant.

Si ce projet de **loi passent**, nous ne **vivront plus** dans le **Canada** mais dans le **Chinada**!!!! Alors je vous invite à **regardé les vrai problèmes** et à **être à la hauteur** des gens qui vous **ont fait confiance** et qui **vous ont élus**.

Merci

Helene Gagné

N.B. Je vais rendre le contenue de ma lettre publique sur les médias sociaux!!!

 From:
 Josie Camblin

 To:
 ICN / DCI (PCH)

 Subject:
 OPPOSE ADDITIONAL CENSORSHIP TO INTERNET

 Date:
 August 1, 2021 12:34:15 PM

#### TO WHOM IT MAY CONCERN:

As a Canadian protected by the Charter of Rights, I oppose any additional censorship to the internet. This infringes on my freedom of speech and privacy and to voice an opinion. It is one-sided and the government has no right to our individual and personal affairs and definitely it has no right to tell us what to think or say or what to believe in. All people should have a choice and a voice and be free to choose for themselves reasonable, unharmful content, what to listen to, what to research, what to question and believe and decide what is harmful or misinformation.

This type of proposed censorship is tyrannical, allows for corruption of big tech and politicians to infringe on our privacies, silences the innocent, controls and separates good people and used by communist countries to silence the people. It is dangerous for a sovereign country and goes against our sovereignty and freedom rights. Every voice needs to be heard and we are all essential. Currently mainstream media is censored and owned by the elite and big tech and has a political agenda that is extremely biased and corrupted.

The people of Canada have a mind and a right to distinguish what is hateful, harmful or lies for themselves. Trudeau and his supporters do not represent the common people, but part of the elite few who have no idea the hardships of the common people. We don't appreciate the invasion of our privacy.

J. Camblin

Sent from my iPad

#### Felicia Mazzarello

From:Nathaniel Rand <</th>s.19(1)Sent:September 26, 2021 2:45 PMs.19(1)To:ICN / DCI (PCH)Subject:Response To Proposed Framework to Address Hateful Online Content

To Who it May Concern,

My Name is Nathaniel Rand, and I write to you as an Information Security Professional and concerned citizen of Canada, regarding the Proposed Online Harms framework.

Below, I outline my concerns regarding this proposed framework.

1. Existing Mechanisms within the Criminal Code allow for the government to enforce the takedown of harmful or otherwise objectionable content. This can be accomplished without creating another Bureaucracy in Ottawa.

2. Law Enforcement Agencies across the country (Locally, Provincially and Federally) will often decline to become involved in matters regarding the non-consensual exchange of intimate images, referring to it as a civil matter. Many provinces have Civil Torts that allow for individuals to seek relief in such cases. Additionally, some provinces such as Nova Scotia, have existing legislation that regulates Cyber-bullying or the non-consensual release of intimate images.

3. Existing Mechanisms require oversight by the Judiciary. There is no such accountability for the propsed Digital Safety Commissioner. Judicial Oversight of a system that imposes penalties is essential. Existing mechanisms within the criminal code that require Judicial Oversight, such as Anton Piller order would fulfil this role.

4. Additionally, Section 89 of the Technical Paper on Online Harms stipulates that an Inspector, may at any reasonable time, inspect any place in which they believe on reasonable grounds that there is any information relevant to verifying purpose of verifying compliance with the proposed act. Mechanisms (Anton Piller Orders) already exist for such an action and must be approved by a Judge prior to being executed. This bill provides no such oversight of the government actions. Any action that enters a premises for the purpose of search, seizure of verification, should be overseen by a member of the judiciary.

5. Should this proposed technical paper become law, many second and third order effects may impact the Canadian Market. Given the onerous regulatory regime that this bill proposes, some technology companies that are based outside of Canada may choose to exit the Canadian market entirely. Additionally, it would have a chilling effect on any start up that may wish to be based in Canada but cannot afford the costs (either monetarily, or in personnel.) to comply with the proposed regulatory regime.

As outlined, this Frameworks has many issues, which come into conflict with the rights and freedoms as outlined in the Charter of Rights and Freedoms, and as such I would ask that this framework be revised and adjusted in order for it to be more in line with the Charter, prior to a bill being introduced in Parliament.

Thank you for your time regarding this matter.

Nathaniel Rand, CISSP

From:	Jean-Charles Tremblay
To:	ICN / DCI (PCH)
Subject:	opinion
Date:	August 1, 2021 11:58:49 AM

Envoyé à partir d'Outlook

pourquoi se mêler de l'opinion des citoyens ....serais-ce pour une orientation différente...et en contrôler le contenu..!

que cet opinion ou orientation venant de citoyens(es) soit inadmissible ou répréhensible pour un et l'autre cela demeure un "opinion" à prendre ou laisser.....il serait préférable de vous orienter vers une "orientation" objective d'une éducation plus représentative d'un pays auquel on veut donner une orientation objective et axé sur des valeurs dont le pays veut se dotter.....!

jean c. tremblay

 From:
 Plerre Graham

 To:
 ICN / DCI (PCH)

 Subject:
 Refus de cette mesure ...!!!

 Date:
 August 1, 2021 11:46:51 AM

Je Refuse d'être censurer d'aucune façons...

ils ne dois se faire que par la discussion et non pas en abrogeant les droits individuels de la personne

Envoyé de mon iPhone

## Felicia Mazzarello

From: Sent: To: Subject: jrempel jrempel September 26, 2021 9:25 AM ICN / DCI (PCH) sharing

s.19(1)

please don't do it

### Felicia Mazzarello

From: Sent: To: Subject: Paul M s.19(1) October 5, 2021 5:54 PM ICN / DCI (PCH) Strong Objection to Proposed Harmful Content Legislation

Speaking as someone in a technical field and with a good understanding of the technology required to enforce the proposal, I must strongly object to the proposed Harmful Content Legislation.

I object both from a technical perspective and an ethical perspective.

I STRONGLY oppose the offloading of enforcement on private companies under the threat of severe financial penalty. The end result would lead to an over-representation of false accusations enforced by these private companies under the fear of not being able to clearly resolve the claim before the 24 hour period expires. This would seriously harm free speech and productive conversation online.

Furthermore, due to the wording and lack of recourse available to those who are wrongly accused or mistakenly have this enforced upon themselves, this system would be absolutely rife with abuse and mis-use for nefarious purposes by private individuals and potential future governments alike.

This is ethically wrong and technologically flawed.

I URGE all those involved to listen to civil liberty advocates, legal authorities, and social media companies regarding their very founded concerns regarding this legislation.

thank you - Paul Mailloux.

 From:
 Hope Blanco

 To:
 ICN / DCI (PCH)

 Subject:
 Censorship

 Date:
 July 31, 2021 8:56:36 PM

I don't approve of your additional censorship of the internet

Sent from my iPhone

Line Savard the Access to
ICN / DCI (PCH)
Approche proposée du gouvernement pour s'attaquer au contenu préjudiciable en ligne
July 31, 2021 6:53:58 PM

Moi, ainsi que toutes les personnes que je connais sommes **totalement contre** cette mesure qui est inacceptable en tous points de vue!

### Felicia Mazzarello

From: Sent: To: Subject: Vladimir Sedach s.19(1) October 5, 2021 4:10 PM ICN / DCI (PCH) The Government's proposed approach to address harmful content online

Hello,

I am writing to strongly oppose the proposed "new legislative and regulatory framework for social media platforms." From the extremely vague language, such as the phrases "terrorist content" and "content that incites violence," it is obvious that this proposal is going to be another tool used by the Federal and provincial governments to target people involved in environmental and animal rights movements, as is currently being done with other legislation around "terrorism" and "incitement of violence."

Why lump all of this in with "child sexual exploitation content," as if there was not existing legislation addressing that issue? This kind of cynical "think of the children" appeal is an insult to one's intelligence, and shows that the people behind this proposal do not even have the guile to run the crude government censorship operation they are proposing.

----

**Vladimir Sedach** 

 From:
 Colette dupuis

 To:
 ICN / DCI (PCH)

 Subject:
 Je suis contre ce projet

 Date:
 July 31, 2021 5:51:57 PM

Envoyé de mon iPad

From:	S Bemier INE ACCESS 10	
To:	ICN / DCI (PCH)	
Subject:	Approche proposée du gouvernement pour s'attaquer au contenu préjudiciable en ligne	
Date:	July 31, 2021 5:33:58 PM	

Bonjour,

Je suis contre. Vous n'avez pas à réglementer et censurer le contenu en ligne. NOUS NE SOMMES PAS LA CHINE (BIEN QUE ÇA SEMBLE ÊTRE LE BUT DE JUSTIN TRUDEAU). Le Canada est un pays libre.

Le but est politique : censurer le discours qui va à l'encontre du gouvernement de Trudeau et ses idées liberticides.

Je suis contre. Laisser la liberté d'expression. Les discours haineux sont DÉJÀ réglementés.

LAISSER LE CANADA UN PAYS LIBRE!

Bye,

 From:
 chris leray

 To:
 ICN / DCI (PCH)

 Subject:
 Honte à vous!

 Date:
 July 31, 2021 4:19:16 PM

Il est inadmissible de censurer le web et les médias sociaux au motif qu'il pourrait y avoir des messages haineux. C est totalement anti-démocratique. Le fait que ça se passe en plein été en est la preuve ultime!

M. Guilbeault et Trudeau sont des traîtres qui livreront à nos enfants un pays dans lequel la liberté d expression ne sera plus qu' lointain souvenir.

Si une personne est heurtée, elle doit porter plainte. Il faut laisser la Justice faire son travail.

Télécharger Outlook pour Android

### Felicia Mazzarello

From: Sent: To: Subject: James Perry October 5, 2021 5:56 PM ICN / DCI (PCH) The Great Firewall of Canada

The harmful content proposal is an unconscionable violation of the basic human rights of all Canadians.

When China started to open itself up to the Internet, it established a series of laws and policies collectively known as the Great Firewall of China, to "protect" its people from all the harmful ideas out there on the internet. China is a totalitarian society known for its lack of respect for basic civil rights. And the imposition of the Great Firewall of China was widely regarded as an oppressive act of an oppressive regime.

The Harmful Content Proposal is little different. It is the Great Firewall of Canada, and the world and history will look upon it as one of the shameful acts of our country's existence. Do not put Canada on the wrong side of basic decency and erode any sort of moral standing our country has as a defender of human rights.

James Perry

s.19(1)

 From:
 Egore Brem

 To:
 ICN / DCI (PCH)

 Subject:
 Proposed Approach

 Date:
 July 31, 2021 2:00:05 PM

The government has no place policing speech on or offline. The proposal is the highest form of human rights violation as it proposes to own and police people's minds and communication.

Silencing political opponents is the first thing that will be done using it.

Look at history and ask yourself when have the authoritarian dictators been on the right side? How many faced prison terms later on for their involvement (staff included)?

Resign.

From:	Cynthia Goodchild
To:	ICN / DCI (PCH)
Subject:	Harmful content online
Date:	July 31, 2021 1:28:34 PM

This or something can't come soon enough. Don't just stop at Twitter, Facebook and You Tube – you need to address the young youth – it all starts there. Instagram is one of the youth's largest platform. Snapchat is another. Yes, hard with direct messaging and trying to govern that – but if these companies aren't held responsible then the youth that turn to be adults will just continue with their attitude that they can take people down with words hidden behind a very powerful computer that can spit hate words, images, terrorist comments in seconds to thousands and then those seem to go instantly to an un quantified number. Then the "me too" movements on whatever is posted goes viral on these sites!!!

The youth have not been taught decorm or to think for themselves.

Something has to be done. The avenue of speaking through this platform is great but what about reaching the youth – reaching out to all Canadians in an easy way....what about getting all to participate.... There must be a way the government can reach out to them and I think you will be surprised to hear their voices and what they have to say and think.

Please move forward as fast as you can on this!!! It will save lives.

Cynthia Goodchild

From:	Austin Yeung (he Acce
To:	ICN / DCI (PCH)
Subject:	Cease the Government's proposed approach to address harmful content online
Date:	July 31, 2021 12:14:30 PM

Hello,

As a Canadian, I am voicing my concern and opposition to this legislative and regulatory framework to online content. This is not Canadian and should never be implemented. Simple as that.

Sincerely, Austin Yeung.

# TekSavvy's Submission to the Department of Canadian Heritage Regarding its Consultation on Internet Harms

## I. Introduction

TekSavvy Solutions Inc. ("TekSavvy") is pleased to submit the following comments in response to the Government of Canada's consultation on its proposed approach to address harmful content online (the "Consultation"). TekSavvy is an independent internet service provider ("ISP") based in Chatham, Ontario, and Gatineau, Quebec. It is Canada's largest independent ISP with a network across Canada and has been providing Canadian consumers with wireline broadband internet services since 2002. In addition to residential and business internet, TekSavvy also offers other telecommunications services such as telephone services and Internet Protocol television through its affiliate, Hastings Cable Vision.

Recognizing that there are public interest groups and researchers with expertise in these types of content and their regulation, TekSavvy seeks to make comments specifically from the narrow perspective of an ISP without commenting on all the broader considerations of the proposal. However, TekSavvy wishes to note that as a long-time champion of net neutrality and freedom of expression, it shares some of the concerns that others have expressed with the proposal. These include that the Consultation does not provide precise definitions for the types of harm or the types of electronic service providers to which it would apply; that it does not reference existing bodies of research on regulating the categories of online harms it addresses and that it is not effective to address all of these varied types of harms in a single piece of legislation.

From the perspective of an ISP, TekSavvy makes these submissions on the following topics:

- Since content moderation as proposed in the consultation would require automated systems, the framework should build on lessons learned from issues with other applications of automated systems for regulatory compliance;
- Since content moderation using automated systems at scale will necessarily involve automated decision-making, the framework should rely on or incorporate the Government's existing tools to evaluate automated and artificial intelligence systems employed for regulatory compliance; and,
- If site-blocking court orders are included in the legislative framework, there should be a clear set of factors or criteria that the court would be required to consider and weigh before issuing an order.

### II. Use of Automated Systems for Regulatory Compliance

Automated processes will lead to over-censorship

The proposed 24-hour window for content moderation decisions, including decisions that would render the flagged content inaccessible in Canada, will almost certainly necessitate the use of automated decision-making. While this window may be appropriate for some types of illegal

content, we expect that applying this window uniformly across all types listed in the Consultation would result in a large degree of over-censorship.

A 24-hour moderation window would appear more achievable and less prone to error for some types of content subject to the proposal, such as child sexual exploitation material or intimate images that are found to be non-consensually shared. First, there are existing methods for automatically identifying copies of images known to fit within these categories. Further, this type of content would appear much less subject to nuance than the other listed categories.

For other types of prohibited content, such as hate speech and content inciting violence, however, there is much more room for the nuances of humour, sarcasm, fair comment, *etc.*—all of which can be expected to be difficult for an automated system to perceive or assess. Litigation that turns on whether something falls into these very categories can result in long court proceedings that reach the Supreme Court of Canada<sup>1</sup>; one could imagine the difficulty therefore in creating an automated system for assessing this type of content with any precision.

As a result, implementing a 24-hour window for making decisions on accessibility for all identified types of content would almost certainly lead to over-censorship. Platforms expected to meet this timeline would have every incentive to allow their automated tools to err on the side of making impugned content inaccessible in Canada in order to avoid incurring penalties for not meeting their regulatory obligations. Put another way, platforms would have every incentive to over-censor and little incentive to carefully consider the legality of content that may be on the fringes.

TekSavvy has experience with the use of automated tools for regulatory compliance through our development of systems for receiving and processing notices of infringement. Under the "notice-and-notice" provisions in sections 41.25 and 41.26 of the *Copyright Act*, <sup>2</sup> ISPs such as TekSavvy are required to forward a notice of infringement from a copyright owner to the subscriber at the IP address listed in the notice "as soon as feasible" once received. Copyright owners are prohibited from including some content, such as demands for payment or personal information, in their notices. The *Copyright Act* currently provides for statutory damages of not less than \$5,000 and not exceeding \$10,000 in the event that an ISP fails to perform its obligations. There is no express provision in the *Copyright Act* allowing for a due diligence defence, with the result that it is unclear if every failure to forward a notice would result in a fine (even where the ISP can show its due diligence).<sup>3</sup>

<sup>&</sup>lt;sup>1</sup> See for example, *R v Keegstra*, [1990] 3 SCR 697 or *Saskatchewan (Human Rights Commission) v Whatcott*, 2013 SCC 11, [2013] 1 SCR 467, both of which discuss the appropriate meaning of "hatred" at some length.

<sup>&</sup>lt;sup>2</sup> Copyright Act, R.S.C., 1985, C-42.

<sup>&</sup>lt;sup>3</sup> We note that this issue may be litigated in the Federal Court as a result of claims of almost \$400 million filed by several copyright holders against Bell Canada for alleged failures to forward copyright notices. See Federal Court Docket T-1062-21, *Millennium Funding, Inc et al v. Bell Canada et al.* 

TekSavvy receives many thousands of these notices on a weekly or even daily basis. As a result, like many ISPs, TekSavvy has developed an automated system for processing these notices, identifying subscribers, forwarding notices to the identified subscriber, and retaining customer information as required. Manual review over all notices it receives would be impossible for TekSavvy. However, TekSavvy's automated process cannot ensure that it does not forward non-compliant notices. Notices containing prohibited content cannot be detected with precision; if TekSavvy used a process by which to flag notices with certain keywords, for example, this would lead to some compliant notices failing to be forwarded. Because of the monetary risk associated with failing to forward notices and the lack of an explicit due diligence defence, ISPs must err on the side of over-forwarding notices to ensure their own regulatory compliance. This means notices that contain prohibited settlement offers or demands for payment, which can be intimidating to customers, continue to be forwarded to customers. This situation is the direct result of the notice-and-notice framework requiring perfect compliance at a large scale concerning imperfectly defined standards.

This can be analogized to the case of platforms, who, in seeking to meet a required 24-hour moderation window, and without a robust due diligence defence, would almost certainly err on the side of over-censoring. While 24 hours may be appropriate for categories such as child sexual exploitation material and sexual images shared without consent, we encourage the use of a longer window of time for other forms of harmful content - such as content suspected of being hate speech, content inciting violence, or terrorist content — to allow platforms a more rigorous and thoughtful review. Further, we encourage the inclusion of an explicit due diligence defence with well-defined criteria. Platforms could show, for instance, that their automated system was developed with diligence and in good faith, continues to be monitored for needed updates, and that it does a reasonable job of meeting the regulatory requirements. For an instance of content that was missed by the system, the platform would then have the ability to explain the criteria of its system to provide a reasonable explanation for the error, if one existed. For example, it would be defensible for a platform to show that it did not use a given criterion in an automated decision-making process because of an internal finding that it led to high instances of over-censoring which outweighed the harms caused by a given category of content.

If not, the risks of over-censorship of legitimate content are real. It could for example result in over-censorship of content from vulnerable or marginalized groups — the very groups the Consultation is in part designed to protect. This content may attract more complaints or "flags" on those platforms simply because of its dissent from opinions of larger groups or because of more targeted attempts to silence certain content. Open and thoughtful discussions from these communities could also use many of the keywords that automated systems use as criteria for taking down content. Examples of these moderation errors include Facebook's deletion of a woman's social media post detailing an experience in which her sons' were called a racist epithet<sup>4</sup> or a Twitter user who took responsibility for reporting sex workers' social media

<sup>&</sup>lt;sup>4</sup> Dwoskin, Elizabeth and Tracy Jan, The Washington Post, "<u>A white man called her kids</u> the n-word. Facebook stopped her from sharing it," 31 July 2017.

accounts until they were shut down.<sup>5</sup> Automated systems required to blindly rely on the number of times content is reported or the use of certain keywords, in order to meet a strict 24-hour window, therefore, can be expected to lead to over-censorship.

### Using Automated Decision-Making for Nuanced Decisions

The large platforms that we understand the Consultation seeks to address have existing content moderation practices in place that generally already use automated decision-making processes. In seeking to move part of these existing content moderation practices into the regulated sphere, the Government ought to ensure that these automated decisions do not serve to exacerbate some of the very issues that the Consultation seeks to address. For example, algorithms have the potential to make decisions based on criteria that have potential unintended biases in a manner that is not transparent to the public. For example, several studies have indicated that artificial intelligence models for processing hate speech were more likely to flag tweets as offensive or hateful when they were written by African Americans.<sup>6</sup>

As a starting point, TekSavvy submits that engaging with the Government of Canada's own *Directive on Automated Decision-Making*<sup>7</sup> and Artificial Intelligence Impact Assessment tool<sup>8</sup> could be a requirement for platforms in developing automated tools for making content moderation decisions. Platforms could also be required to provide transparency as to the criteria used in their automated decision-making, whether to the public or to the Government.

## III. Considerations for Site-Blocking Orders

The Consultation proposes to provide the proposed Digital Safety Commissioner of Canada with the power to apply to the Federal Court for an order to require Telecommunication Service Providers to block or filter access to a service that has repeatedly refused to remove child sexual exploitation and/or terrorist content. We are pleased with the qualification in the Discussion Guide of this potential tool as an "exceptional recourse," the proposed judicial oversight over such orders, and the limited application to providers with violations regarding two of the five types of content (child sexual exploitation and/or terrorist content) as opposed to all forms of content the Consultation intends to address.

TekSavvy is of the view that site-blocking as an enforcement tool is generally simultaneously overly broad (as a result of the real risk of blocking legitimate content) while also ineffective. The only form of site-blocking that has been used in Canada to date requires ISPs to block access to specific domain names by removing those domain names from the ISP's domain name system (DNS). This is trivial to circumvent by the use of an alternative DNS service, many of which are

<sup>&</sup>lt;sup>5</sup> Clark-Flory, Tracy, Jezebel, "<u>A Troll's Attempt to Purge Porn Performers from</u> Instagram," 17 April 2019.

<sup>&</sup>lt;sup>6</sup> Ghaffary, Shirin, Vox, "The algorithms that detect hate speech online are biased against black people," 15 August 2019.

<sup>&</sup>lt;sup>7</sup> Government of Canada, <u>Directive on Automated Decision-Making</u>, 1 April 2021.

<sup>&</sup>lt;sup>8</sup> Government of Canada, <u>Algorithmic Impact Assessment Tool</u>, 1 April 2021.

freely available and that many internet subscribers already use without the goal of circumventing site-blocking. Even more sophisticated forms of site-blocking can be easily circumvented by those with only a moderate level of technical knowledge. Presumably the very persons seeking to access this type of content would be those most motivated to research and employ the fairly simple means of circumventing site-blocking mechanisms.

With that said, should the Government determine that site-blocking repeatedly non-compliant platforms could in some circumstances be an effective enforcement tool in incentivizing those platforms to comply (rather than for the block's purported efficacy in blocking access to content), we suggest that such an extraordinary remedy should only be available where it outweighs countervailing interests. To evaluate when that is the case, the statutory scheme ought to include certain criteria that courts would be required to consider in issuing such orders. We would suggest that these criteria include:

- Instrument of last resort. As recognized above, the site-blocking injunction should truly be an "exceptional recourse." In seeking an injunction, the Government should be required to demonstrate that it has sought other avenues of enforcement in order to reserve site-blocking for only those limited cases where other attempts have been unsuccessful. Put another way, the court ought to be convinced that alternative and less onerous measures were not effective. This would help ensure that site-blocking orders do not become a default enforcement mechanism but are instead reserved for extraordinary cases. Given ISPs' obligations not to discriminate against any traffic as a result of section 36 of the *Telecommunications Act*, <sup>9</sup> it is important to take measures to ensure that site-blocking is only used as an instrument of last resort.
- Balance of freedom of expression considerations. The Court should weigh the public interest in access to the platform in question against the enforcement considerations. This should include consideration of the degree to which Canadians' access to and engagement with legitimate content would be affected. There may, for example, be international platforms that are outside the traditional enforcement reach of the Canadian Government (absent international cooperation) and that do not consider Canada an important jurisdiction relative to their total user base. Other enforcement efforts against such platforms may therefore not have worked and the platforms may not have taken steps to meet Canadian regulations as a result of the small size of the jurisdiction. However, the platforms may still have other self-moderation policies in place that simply do not meet the criteria of the Canadian regime. The court should consider the effect of Canadians' loss of access to a platform of this type against the severity of the platforms' non-compliance. As an analogy, news media company CNN took the decision to withdraw its social media presence in Australia owing to Australia's decision to impose liability for defamatory comments on Facebook pages.<sup>10</sup> This result deprives Australians of access to legitimate content to which they otherwise would have access, which may

<sup>9</sup> Telecommunications Act, S.C. 1993, c.38.

<sup>&</sup>lt;sup>10</sup> B&T Magazine, "US News Giant CNN Restricts Access To Facebook Pages In Australia Following High Court Ruling," 29 September 2021.

seem to be an outsized effect compared to the seriousness of defamatory comments on Facebook pages.

- Technical clarity. The statutory scheme should be clear with respect to the technical type of blocking that is required of ISPs, rather than suggesting ISPs use whatever means necessary to block a website. For example, as described above, to date the only form of site-blocking in Canada has been DNS de-indexing. However, it is easily circumvented through various technical workarounds, including the use of alternative freely available DNS servers or VPNs. Despite these possible circumventions, the statute should be clear that ISPs are not required to take additional, more invasive blocking steps that impose even greater burdens on ISPs. For example, IP blocking can affect unrelated internet resources beyond the site the blocking is intended to affect, and will impose higher operational costs to implement, maintain and trouble-shoot. Blocking based on content or specific protocols would require deep packet inspection, an invasive and advanced type of monitoring network traffic that would impose highly burdensome monitoring requirements on ISPs, would require specific equipment, and entail violations of the privacy of customers. The statute should be clear which type of blocking is required of ISPs, to promote certainty for ISPs and avoid incurring liability for not taking all possible blocking steps.
- Clarity as to which party has the obligation to update the list of blocked sites. As noted above, site-blocking carries a real risk of blocking legitimate content and stifling freedom of expression. It also is ineffective when websites are simply able to reappear under new domains or IP addresses. As a result, any list of domains subject to a blocking order will almost certainly need to be revised for currency and accuracy. The statutory regime should clarify that ISPs are not responsible for maintaining the list or liable for any inadvertent blocking of legitimate content. Instead, the Government must take reasonable steps to ensure that the list remains accurate (*i.e.*, including seeking revised court orders) and to identify issues of inadvertent blocking.
- Consideration of the burden imposed on the ISP. The scheme should expressly
  require the court to consider the burden that the injunction would impose on the ISP,
  including the aggregate effect of the injunction together with any other site- and
  application- blocking injunctions in effect for that ISP, as well as the technical feasibility
  and effectiveness of the proposed blocking in addressing the infringement.

# IV. Conclusion

TekSavvy appreciates the opportunity to provide its comments on the Consultation. TekSavvy would be in favour of distinct regimes that are specific to the types of content at issue, based on the existing body of research on enforcement of these types of illegal content, and which engage in detail with the definitions of the harms at issue as well as technical details that will have significant bearing on the success of the regime. TekSavvy also reiterates the importance of issuing site-blocking orders only where prescribed statutory criteria are met.

Given these concerns, TekSavvy believes that the current proposal needs to be further developed and that more processes to consult on future developments and refinements are

required. We hope for more opportunities to participate in providing feedback as the discussion of online harms advances.

 From:
 Greg Jeffrey

 To:
 ICN / DCI (PCH)

 Subject:
 Bill C-36

 Date:
 July 31, 2021 11:55:52 AM

As someone who grew up being bullied.

This is not the right approach.

Not sorry.

 From:
 Diane Arel

 To:
 ICN / DCI (PCH)

 Subject:
 Liberté d''expression

 Date:
 July 31, 2021 11:23:47 AM

Je suis née au Canada, non pas au Chi-nada !!!

Envoyé depuis ma tablette Samsung

From:	Elizabeth Robinson
To:	ICN / DCI (PCH)
Cc:	MP Julie Dzerowicz
Subject:	The Government's proposed approach to address harmful content online
Date:	July 31, 2021 10:22:21 AM

I am writing in response to Canadian Heritage's technical paper proposing a new legislative framework to address harmful content online.

I am strongly opposed to The Act proposed in this paper. It is straightforwardly a proposal of censorship that will curtail the civil liberties of people residing in Canada while doing nothing to make them safer.

To briefly list some key concerns:

(1) The proposed Act indicates that the kinds of harmful content it hopes to address are already covered by the Criminal Code. If this content is already illegal it is not clear what further protections are being added by the Act. I can only assume that the Act covertly serves a larger agenda of government control and censorship over online content.

(2) The proposed Act will define "terrorism content" as "content that actively encourages terrorism and which is *likely to result in* terrorism." "Content that incites violence" is similarly defined as "content that actively encourages or threatens violence and which is *likely to result in* violence." The standard of "likely to result in..." is horrifyingly vague. By what possible means can you reasonably judge in advance what content is "likely to result in" violence or terrorism? The Act plans to determine in advance of crimes what crimes are going to take place. This can only result in declaring people criminals before they have committed any crime. The mechanisms of the proposed act create a huge and alarming opportunity for violations of the civil liberties of people residing in Canada. The Act proposed should not more forward at all, but any version that does **must** amend this deeply troubling language.

(3) The proposed Act is based on the premise that "the hatred spread online often has a disproportionate impact on women, Indigenous Peoples, members of racialized and religious minority communities and on LGBTQ2 and gender-diverse communities and persons with disabilities." While true, what the technical paper fails to mention is that these same groups are also the ones disproportionately impacted by online censorship. Creating additional tools to censor content online will disproportionately impact the abilities of persons belonging to these groups to engage in free expression online. As with any system of censorship, abuse of the system and mislabeling of content that does not meet the outlined standards for harm is inevitable. This legislation will disrupt the ability of those with marginalized voices to have a chance to be heard. This is not a theoretical concern, regular censorship of this nature is already happening on the platforms of large online communication services such as Facebook or Instagram.

There are many other concerns one could raise about the proposed Abc, but the concerns raised above should be sufficient to show that the Act as proposed should not move forward.

Sincerely, Elizabeth Robinson

 From:
 Sébastien Champagne

 To:
 ICN / DCI (PCH)

 Subject:
 Mon opinion

 Date:
 July 31, 2021 10:00:20 AM

Merci de nous permettre de nous exprimer. Cependant, je ne crois pas que vous êtes sincères dans votre démarche. Avec toutes les manipulations de chiffres et la censure depuis plus d'un an, j'ai perdu le peu de confiance qu'il me restait envers mon gouvernement.

Envoyé de mon iPhone

From:	Josee B (In E. ACC	
To:	ICN / DCI (PCH)	
Subject:	Plateformes de médias sociaux et autres services de communication en ligne	
Date:	July 31, 2021 8:25:20 AM	

Bonjour,

Je vous écris pour vous signifier mon désaccord avec le nouveau cadre législatif et réglementaire qui créerait des règles sur la manière dont les plateformes de médias sociaux et autres services en ligne doivent traiter les contenus préjudiciables que vous proposez. Vous nous prenez pour des imbéciles en proposant encore des lois extrêmement liberticides sous couvert de protéger les utilisateurs.

Arrêtez de nous infantiliser et ne nous croyez pas dupes de votre agenda mondialiste. Nous ne sommes pas d'accord avec vos plans pour la nouvelle normalité.

J'espère que notre avis sera pris en considération même si j'en doute fortement vu l'absence de démocratie depuis 16 mois dans ce pays.

Bien à vous,

Josée Baldassarre

#### s.19(1)

From:	and the second se
To:	ICN / DCI (PCH)
Subject:	Nouvelle loi sur la censure en ligne.
Date:	July 31, 2021 7:52:38 AM

Bonjour !

la Loi sur l'accès à l'information. Document released pursuant to the Access to Information Act.

Document communiqué en vertu de

En tant que je suis favorable à ce que des sanctions ou des amendes soient appliqués à des gens ou des groupes qui distribuent des images pédopornographiques, aux pirates informatiques, aux terroristes ou gens qui font circuler des idées islamistes ou intégristes musulmanes, aux gens qui font la promotion du racialisme et du racisme en faisait référence aux différences morphologiques des humains pour établir des politiques discriminatoires. Même les sites qui encouragent l'adultère, comme les sites de rencontre pour gens mariés, devraient être fortement surveillés et même interdits, en considérant les dommages que ceux-ci causent dans le tissu social.

Il serait important de clarifier la définition de «haineux» dans votre nouvelle proposition de loi pour ne pas faire le jeux des islamistes, des racialistes ou des néo-nazis par exemple.

Par ailleurs, donner des pouvoir supplémentaires à la commmission des droits de la personne ne me semble pas sage, puisque celle-ci favorise la discrimination basée sur l'apparence des gens, ce qui va à l'encontre de la cohésion sociale.

Veuillez, mesdames et messieurs, agréer l'expression de mes sentiments les meilleurs.

-Sébastien Lépine

Envoyé depuis mon appareil Galaxy

 From:
 Christian Breton

 To:
 ICN / DCI (PCH)

 Subject:
 Bonjour,

 Date:
 July 31, 2021 6:36:14 AM

Je crois que le fait de censurer les gens va à l'encontre de la liberté d'expression et de la Charte des Droits et Libertés ainsi que des Droits de l'homme. Cela semble totalement inacceptable.

C. Breton

Provenance : Courrier pour Windows 10

#### Avis de confidentialité :

Ce message et toute pièce jointe sont la propriété du Centre de services scolaire des Samares et sont destinés seulement aux personnes ou à l'entité à qui le message est adressé. Si vous avez reçu ce message par erreur, veuillez le détruire et en aviser l'expéditeur par courriel. Si vous n'êtes pas le destinataire du message, vous n'êtes pas autorisé à utiliser, à copier ou à divulguer le contenu du message ou ses pièces jointes en tout ou en partie.

nadia dicaire
ICN / DCI (PCH)
Non a cette censure
July 31, 2021 4:54:48 AM

Je suis tout à fait contre votre projet Laissez nous nous exprimer

À quoi jouez vous depuis quelques temps

Vous êtes qui pour décider à notre place de ce que nous pouvons penser ou dire. Tant qu'il n'y a pas menace de mort, menace de faire du mal à quelqu'un je crois et je soutiens la liberté d'expression. Et je refuse catégoriquement, de vous donner ce pouvoir vous avez causé assez de tort au canadien depuis un certain temps. J'aimerais que vous quittiez-vous tous!! vos postes parce que vous ne nous représentez plus! Vous représentez une force démoniaque et c'est vous qui êtes dangereux pour nous. #noussavons ce qui se passe, nous savons que vous voulez gouverner en dictateur. Et nous savons que vous promettez, des plans désastreux pour le peuple. Et je souhaite que votre plans échoue avec tout mon coeur, toute mon âme et mon esprit aussi. Je suis souveraine et j'aimerais mieux mourir que vivre dans un monde comme vous le dessiner. Votre monde de fausse paix, où vous protéger vos avoir sur le reste de la population. Un monde ou vous encore une fois assoyez votre noir pouvoir sur le peuple. Un monde plus mauvais, plus nauséabond, un monde qui vous ressemble!! Mais je ne suis pas de ce monde alors je refuse vos manigances. Vous êtes des êtres plutôt grotesques et abjectes. Et attention, je ne positionne pas en victime ici non parce que je sais qui vous êtes. Des êtres malveillants au coeurs plus que noirs. Je refuse de faire affaire avec vous. Je ne vous doit rien. Vous avez laisser votre conscience au diable, et ils vous a pourris de l'intérieur! Mais un jour la lumière brûlera ceux qui abuse des autres et quand ce jour viendra justice sera faite.!!!

Je suis contre votre projet de loi aucune censure sur les médias sociaux !!

Télécharger Outlook pour Android

From:	Aria Motazedi
To:	ICN / DCI (PCH)
Subject:	Internet Censorship
Date:	July 31, 2021 3:22:28 AM

Hello,

I am Aria Liam Mehrdad and I would like to let the Canadian Government know that I am disappointed about this bill that will censor free speech on the internet.

He came to Canada to build a better life and to simply have freedom. This bill is a huge spit to his face, to his family and to every Canadian out there that want to be able to have freedom of speech. Freedom unites everybody but dictatorship type of bills will only divide Canadians. If the Government prefers censorship over freedom, then Canada is no different then China, Iran, North Korea, Cuba, and many other countries that run by dictatorship. Canada can do way better then this horrible bill and if you pass this bill then that means my father's escape was pointless and meaningless because of this bill. He wanted us to live a better life in Canada but that can't happen if this bill is passed!

Best regards

Aria M

 From:
 Bradley Jones

 To:
 ICN / DCI (PCH)

 Subject:
 Input

 Date:
 July 31, 2021 2:33:22 AM

### To Whom It May Concern:

I very strongly support the proposed approach to address harmful content online.

Sincerely, Brad Jones

 From:
 Alain Girard

 To:
 ICN / DCI (PCH)

 Date:
 July 31, 2021 1:21:36 AM

Je suis en total désaccord avec ce projet de loi, une entaille très grave dans la démocratie.

 From:
 boomsday

 To:
 ICN / DCI (PCH)

 Subject:
 Censorship

 Date:
 July 31, 2021 12:24:22 AM

Censorship is an inherent moral wrong and every politician supporting it should be barred from office for violating the fundamental freedoms section of the constitution.

From: To: Subject: Date: Lucie Fortin ICN / DCI (PCH) Demande de participation au projet de loi visant à lutter contre la violence en ligne July 30, 2021 8:13:39 PM

Bonjour,

Je vous écris pour vous faire part de mon intérêt à participer au projet de loi pour lutter contre la violence en ligne. Étant d'abord femme, j'ai reçu un nombre élevé de photo de sexe masculin nu non sollicité. Les messages à caractère sexuel, aussi non sollicités, font partie de ma réalité. Je subis aussi l'ignorance du public lorsque je travaille puisque mon emploi consiste à gérer des plateformes de médias sociaux.

Selon mon expérience, j'en suis venue à me dire que les plateformes sociales devraient avoir des règlements plus stricts afin de pouvoir tracer les personnes fautives. On se fait souvent dire que les gens se sentent en contrôle, car ils sont « cachés derrière leur écran ». Je suis aussi d'avis que les dirigeants des plateformes ont de grandes responsabilités à prendre et vous pouvez compter sur mon appui de citoyenne numérique pour faire avancer le projet de loi.

C'est la première fois que je m'implique de cette façon. S'il y a quoi que ce soit d'autre que je puisse faire afin que le dossier soit mis de l'avant, simplement m'en informer.

Amitiés, Lucie Fortin

 From:
 Sonia Morin
 Ine Access to Informati

 To:
 ICN / DCI (PCH)

 Subject:
 À vous la parole : Approche proposée du gouvernement pour s'attaquer au contenu préjudiciable en ligne

 Date:
 July 30, 2021 7:37:59 PM

Le temps des Nazis est terminé!

Je ne veux pas encore de cette attaque liberticide!

Sonia Morin

 From:
 Gail Burgin

 To:
 ICN / DCI (PCH)

 Subject:
 Full support for this

 Date:
 July 30, 2021 7:33:23 PM

As a victim of cyber stalking our family found out first hand how little support and resources are available. Even police don't seem to have the information required to manage and navigate your way through the help lines and chats of the big tech companies to report stalking via their platforms.

Yes please we need legislation.

Gail Burgin

s.19(1)

Sandy
ICN / DCI (PCH)
Censorship
July 30, 2021 6:44:19 PM

I oppose any censorship that curtails free speech. I oppose any political party putting artificial contraints on its citizen by curbing what they can or cannot say.

We live in a free society where we can express our anger, frustration or opposition to a particular political philosophy.

Without opposition, the Nazi party took control of a whole nation, resulting in milliions of deaths. The same can be said about the murderous socialist regimes in the Soviet Union and China.

We must have a free dialog with our fellow man. Putting artificial laws in place to stop that is diabolical. Do so at your political peril.

Brian Lager

s.19(1)

 From:
 Michel Duguay

 To:
 ICN / DCI (PCH)

 Subject:
 Non mêler vous de vos affaires

 Date:
 July 30, 2021 5:09:56 PM

Votre niveau de jugement et surtout d'intégrité et quasi inexistant

Jamais je ne vous autoriserer à censurer ce qui ne vous plaît pas

Votre hypocrisie est franchement dégueulasse

Rechanger vos règlement CRTC pour que les mensonges médiaditique redevienne illégaux

Bien à vous

 From:
 Maryse Brochu

 To:
 ICN / DCI (PCH)

 Subject:
 Commentaires sur ce projet

 Date:
 July 30, 2021 5:07:28 PM

Bonjour,

Voici les raisons pour lesquelles je ne suis pas d'accord mais pas du tout.

1. Ce que moi je considère très justifié de publier, vous M. Trudeau vous voulez le censurer.

2. Ce projet va faire en sorte qu'énormément d'informations ne seront pas distribués afin d'informer le public comme ce qui se passe pour la Covid où les vaccins. Vous décidez ce qui est bon ou mauvais au lieu de laisser d'autres scientifiques donner leur opinion et ainsi laisser la personne prendre une décision en toute connaissance de cause. Je vous rappelle qu'il y a que 0,04% de décès dûs à la Covid dont la plupart étaient des personnes âgées ou avec comorbidités et de plus, certaines de ces personnes seraient encore en vie si ce n'aurait pas été qu'on les ait laisser mourrir de solitude et si ont les aurait soigné avec de l'ivermectine.

3. Alors la prochaine catastrophe qui sera provoquée par vos propres expériences sur le climat, encore une fois QUE vos experts payés des fortunes pour mentir pourront donner des informations.

4. Vous utiliser MES impôts pour faire toutes ces expériences, pour créer des Camps Covid, de la publicité mensongère et en plus vous voudriez qu'on écrivent des poèmes de calinours!!!

5. De plus, cette étude est payée aussi pas mes impôts!!

6. CELA SUFFIT!!!

Arrêter cette étude right now et laissez nous nous exprimer!!!

Maryse Brochu

Envoyé de mon iPhone

From:	Valerie Demers
To:	ICN / DCI (PCH)
Subject:	Contenu en ligne
Date:	July 30, 2021 3:59:36 PM

Bonjour,

En tant que citoyenne, je refuse toute loi supplémentaire pour encadrer le contenu en ligne.

Il y a assez de lois déjà existantes.

Que ceux qui ne peuvent tolérer les discours "dissidents", contraire à leur idéologie/religion ou les insultes quittent les réseaux sociaux ou évitent ceux qui ne leur plaisent pas. Ça s'appelle la maturité.

Je suis tout à fait contre la loi C10 ou C36. Juste le fait de vouloir présenter ce genre de loi est inadmissible. Ce n'est pas en censurant des discours qu'ils disparaîtront. Nous ne sommes pas en Chine.

Merci

 From:
 René Chabot

 To:
 ICN / DCI (PCH)

 Subject:
 Non à cette dictature

 Date:
 July 30, 2021 2:26:35 PM

Votre projet de dictature pour le nouvel ordre mondial totalitaire comme la chine c'est NON ...

Envoyé depuis mon appareil Galaxy

 From:
 Marcus Maltais

 To:
 ICN / DCI (PCH)

 Subject:
 Loi woke

 Date:
 July 30, 2021 1:55:09 PM

## Projet de loi inacceptable !

Envoyé depuis mon appareil Galaxy

 From:
 christine therrien

 To:
 ICN / DCI (PCH)

 Subject:
 Opinion

 Date:
 July 30, 2021 1:42:40 PM

Je suis contre la censure internet, vous êtes à l'opposé de la démocratie et ne méritez pas votre poste, PERSONNE.

Vous êtes coupable de tout ce qui arrive.

Aucunement le droit de changer la charte des droits et libertés de la personne, démissionnez!!

#### **Christine Therrien**

 From:
 Guylaine Lacerte

 To:
 ICN / DCI (PCH)

 Subject:
 Je dis NON

 Date:
 July 30, 2021 1:26:29 PM

Je dis NON a votre culture d'annulation et NON a la censure. OUI a la liberte de parole et OUI a la democratie et NON au communiste. Guylaine Lacerte

From:	Virginie Daras the Abcess to Information
To:	ICN / DCI (PCH)
Subject:	À vous la parole : Approche proposée du gouvernement pour s'attaquer au contenu préjudiciable en ligne
Date:	July 30, 2021 1:08:42 PM

À qui de droit,

J'ai des préoccupations sérieuses à propos de la censure d'inspiration communiste que vous essayez d'implanter. Je trouve cela complètement inacceptable et contre tous les droits fondamentaux de notre démocratie. Vous êtes en train de revendiquer la censure contre les canadiens. L'internet "woke" qui glorifie la culture d'annulation des partis politiques des Libéraux, NPD, Vert et du Bloc n'est qu'un outil de division sociale mondialiste.

Déjà que vous êtes complètement inactifs, silencieux et complices avec ce qui se passe comme scandale de cette fausse pandémie, vous voulez davantage nuire à la liberté d'expression des canadiens. Vous êtes une honte pour notre pays et pour vos enfants et nos futures générations.

Au Québec, on dit bien, "je me souviens"...Continuer votre division et votre agenda communiste. Le peuple se souviendra aux élections de la trahison que vous avez commise envers notre beau pays.

Seuls les gens qui ne se font pas manipuler, qui ont assez de courage pour se tenir debout contre vos lois liberticides, nous sortirons de cette ...merde... (il n'y a pas d'autre mot) que vous voulez nous imposer. J'ai honte de nos gouvernements!

D'une mère qui pensent à l'avenir de tous les enfants,

Virginie Daras Citovenne. électeur s.19(1)

From:	Joey Cayanan
To:	ICN / DCI (PCH)
Subject:	Feedback for Online Hate Measures
Date:	July 30, 2021 1:06:58 PM

#### Hello,

I hope you are doing well. I found out about this inquiry of feedback on the regulation of online hate speech through an article on the Globe and Mail.

My one concern for this regulation of online hate speech is the defining of what constitutes hate speech. A conservative may view certain speech hateful, while a liberal may not (and vice versa). For example, if a conservative speaks out against transgenderism, liberals may define that as hate speech while conservatives would not; and if a liberal speaks out against the state of Israel due to their occupation of Palestinian lands, conservatives may define that as anti-semetic hate speech while liberals would not.

I hope that this regulation of online hate speech is as apolitical and objective as possible in order to differentiate between well-meaning public discourse of sensitive topics and genuine hate speech. Therefore, I urge Canadian Heritage to better define what hate speech is in order to maintain the fundamental canadian value of freedom of speech & expression, while also making all Canadians feel safe and welcomed in our great country.

Joey Cayanan

s.19(1)

 From:
 danielle geoffroy

 To:
 ICN / DCI (PCH)

 Subject:
 commentaire pour contenus préjudiciables

 Date:
 July 30, 2021 1:05:31 PM

Bien sur qu'il a des contenus préjudiciables, mais cette proposition n'est pas acceptable les réseaux doivent rester libre, car ce sera la porte ouverte à la censure, sans mesure, lorsqu'il y a des sites dangereux, alors les services de polices doivent gérer cela, donc pas besoin de votre loi pour ça ! C'est mon opinion,

Bonne journée Danielle Geoffroy

From: To: Subject: Date: Luc Groleau ICN / DCI (PCH) Digital Citizen Initiative July 30, 2021 12:18:58 PM

Hello,

Our story of defamation attacks is so important that we made the front page of The New York Times on January 31, 2021 (Guy Babcock is my brother-in-law):

https://www.nytimes.com/2021/01/30/technology/change-my-google-results.html

The New York Times printed a follow-up article on how slander sites function: https://www.nytimes.com/interactive/2021/04/24/technology/online-slanderwebsites.html

Additional news outlets have printed articles about us:

Toronto Sun: https://torontosun.com/news/local-news/mandel-serial-cyber-stalker-canthide-behind-her-screen-anymore

The Times (London, England): https://www.thetimes.co.uk/article/father-powerless-to-get-online-smears-removed-wgzmsf3f2

La Presse: https://www.lapresse.ca/actualites/2021-03-07/diffamation-sur-l-internet/une-toile-de-mensonges.php

Bay Today: https://www.baytoday.ca/local-news/travis-alkins-among-150-internetharassment-victims-in-ground-breaking-court-case-3466817

Hamilton Spectator: https://www.thespec.com/news/hamilton-region/2021/03/09/cyberstalker-nadire-atas-targeted-dozens-of-hamiltonians-in-vicious-decades-long-smearcampaigns.html

New York Times Podcast: https://www.nytimes.com/2021/04/06/podcasts/the-daily/avast-web-of-vengeance-part-1.html

Vice Media: <u>https://www.youtube.com/watch?v=xfEqfLL7E6M&ab\_channel=VICE</u> The News Forum (Canadian Justice): <u>https://www.newsforum.tv/videos/canadian-justice-what-do-you-do-if-someone-is-defaming-you-online</u>

Some of the above stories were reprinted throughout the world:

New Zealand (https://www.nzherald.co.nz/world/a-vast-web-of-vengeance-whenonline-lies-destroy-lives/AYYDX5NJQEIKPOGDZPWZTGA2GA/) Nigeria

Ireland (https://www.thejournal.ie/sitdown-sunday-longread-5-5344209-Feb2021/) France

Document communiqué en vertu de la Loi sur l'accès à l'information. Document released pursuant to

Mexico (https://laverdadnoticias.com/mundo/Mujer-de-60-anos-termina-presa-por-DIFAMAR-a-sus-enemigos-en-redes-sociales-20210210-0254.html) Brasil (https://istoe.com.br/mulher-e-presa-por-difamar-dezenas-de-pessoas-nainternet/) Israel (https://www.themarker.com/wallstreet/premium-MAGAZINE-1.9511742)

I would like to have an opportunity to be heard in preparation for the proposed law C-36. I am (but speaking on my own behalf and not as an employee of

I wrote software to track posts about our large group and I'm familiar with how the predatory sites work as I monitor over 100 such sites daily. I can also provide my personal insight on how existing Canadian laws are ineffective at helping victims and the impacts of internet harassment and defamation.

I'm located but would agree to travel anywhere or to appear via video to discuss my experiences and thoughts.

Thank you,

s.19(1)

Luc Groleau

From:	Craig Stokes
To:	ICN / DCI (PCH)
Subject:	No to Bill C-36 & C-10
Date:	July 30, 2021 12:13:41 PM

This is a gross and disgusting misuse of government power. Bill C-10 & C-36 goes against our Canadian fundamental rights mentioned in the Canadian Charter of Rights. Just because the intentions are good doesn't mean it's actually a good idea. Bill C-10& C-36 paves way to use the bill to control the truth. Step 4 to becomming a tyrant is censorship and controlling the media and truth.

The wording in the bill is too vague and overreaching. The ability for someone that feels offended to sue someone else anonymously for \$20,000 and be fine up to \$50,000 and up to 12 months in jail is disgusting. The bills are all about feelings with no logic to back it up. This is criminalizing all Canadians just for speaking and promtes people to not speak out about the governments misuse of power or irresponsible spending etc..

This will also help create Canada into a prison state and waste tax payer money monitoring and imprisoning good law abiding citizens just for speaking out about corruption and penalize whistleblowers.

Canada is supposed to be a democracy and is now under threat because of Bill C-10 and C-36. Content reported by randome uses must be taken down in 24 hours by the platform. This is over censorship, how cam we trust random Internet users to be judge and jury on what content is deemed illegal? Most Canadians don't even know the moat simple and common laws, they have no right being a Internet censorship judge and neither does the government.

Freedom of expression opens discussion while censorship closes it all off.

Freedom of speech and expression is just that, we should not be afraid to speak in our country. This freedom is what made our great country.

Passing Bill C-36 & C-10 sets up Canada to start becoming a dictatorship.

Completely reject both bills.

s.19(1)

 From:
 Claude Paradis

 To:
 ICN / DCI (PCH)

 Subject:
 Le projet de loi sur les plateformes numériques

 Date:
 July 30, 2021 12:03:13 PM

Bonjour,

D'emblée, je veux vous remercier de travailler à la préparation d'un tel projet de loi.

J'ai œuvre a la libre circulation de la creation et des idees, mais dans un contexte ou la critique et le travail d'édition viennent assurer une modération. Je trouve que c'est justement ce qu'il manque sur les réseaux sociaux, où tout et n'importe quoi se disent! Encadrer n'est pas de la censure, c'est simplement fournir des balises pour assurer un discours sain, une communication respectueuse.

Je vais consulter les documents que vous mettrez à la disposition et verrai si je peux émettre des commentaires plus précis. Mais je voulais immédiatement vous communiquer mon appui à un tel projet de loi.

**Claude Paradis** 

From:	Spencer Welland
To:	ICN / DCI (PCH)
Subject:	Censorship of online content
Date:	July 30, 2021 10:56:15 AM
	30, 50, 2022 20,00,2070

Censorship of this kind is the top of a very slippery slope. Who is the arbiter of what is acceptable? How do you ensure fairness and balance? How can you ensure that the political class won't use it as a tool to silence their critics?

What about Human Rights Commissions (which I heartily disagee with)? Do they not stand as an arbiter of al, things hateful and if not then they should be disbanded? And finally I believe I am correct in stating that Canada already has laws governing hate speech and as such we do not need this layering on of additional bureaucracy.

Sara Welland

 From:
 Thierry Herrmann

 To:
 ICN / DCI (PCH)

 Subject:
 consultation pour réglementer les réseaux sociaux

 Date:
 July 30, 2021 8:14:41 AM

Bonjour,

je vous ecris pour vous apporter mon soutien total a ce projet de reglementation. Il est temps de mettre fin au pouvoir absolu des geants de l'internet qui peuvent briser des vies par leur inaction.

Merci.

Thierry Herrmann s.19(1)

From:	christiane knupp the Access to 1
To:	ICN / DCI (PCH)
Subject:	Approche proposée du gouvernement pour s'attaquer au contenu préjudiciable en ligne
Date:	July 30, 2021 7:47:21 AM
Date:	JUIY 30, 2021 7.47.21 AM

Je suis entièrement d'accord avec cette proposition du gouvernement Trudeau....Il est grandement temps que les médias sociaux soient étroitement surveillés et qu'ils acceptent la responsabilité de leurs contenus.

Le fait que le Parti Conservateur planifie de s'opposer au projet mentionné ci-haut est tout simplement incroyable!!

Provenance : Courrier pour Windows 10

 From:
 Barb MacKenzie

 To:
 ICN / DCI (PCH)

 Subject:
 C 36

 Date:
 July 30, 2021 6:15:07 AM

Canadians will never agree to this. Period.

B. MacKenzie Taxpayer

From: To: Subject: Date: Laurence I/DE JADCESS 101 <u>ICN / DCI (PCH)</u> My Comments about the government's proposed approach to address harmful content online July 30, 2021 2:28:40 AM

Thank you for the opportunity to provide you with my thoughts on the online harms bill and how I believe it will affect Canadian society.

The comments that I am providing are from the perspective of an everyday Canadian. I am someone who is not a stakeholder and has been following the government's approach to internet regulation closely. I think it is important that the government has a willingness to listen to the perspective of not just industry players but also everyday Canadian's as well who have different views on this issue and use the internet daily for many different reasons as the internet has become an essential part of everyone's life.

I have concerns with the mandated website blocking conceived to protect Canadians from what the government's proposed regulatory regime deems harmful or inappropriate online content. I believe this aspect of the bill could be abused. Over time it could lead to the expansion of the scope of content blocking influenced by lobbyists demanding so from the government for reasons other than what this bill is designed to do. This would not be in the best interests of Canadians.

An example of these lobbyists would be those from the telecom companies such as Bell, Rogers and Telus. They have been clamouring to implement website blocking across the country to serve their own interests. As well, costs for consumers will increase due to the implementation and maintenance of the web-blocking system. Website blocking could also result in the arbitrary blocking of legal content.

24-hour takedowns of online content could lead to legal content being taken down, hurting freedom of speech and expression due to compelling social media sites or websites to remove online content too quickly. Depending on the scenario, this may not allow the content to be properly assessed thoroughly and thoughtfully enough whether it is harmful based on the proposed regulator's criteria of what will be illegal content.

People's personal information could be susceptible to abuse or mishandling, putting their privacy at risk. The government will order social media platforms to provide sensitive subscriber and user information without requesting a warrant which is troubling and lacks transparency.

The Digital Safety Commissioner and Digital Tribunal is the new regulatory regime outlined in the online harms bill. It's the new Bureaucracy involved in content takedowns and policing the internet. The definition of harmful content applies to the main categories of content, which inciting violence, hate speech, intimate images shared non-consensually, and child sexual exploitation content.

There are already laws that can deal with harmful content and discern

between what is and is not illegal. Having a new regulatory body decide this and changing criminal law and other proposed changes such as the CSIS Act to conform to the new regulatory regime seems unnecessary. Creating this new Bureaucracy and making many other changes is like taking a sledgehammer to an issue of concern, social media and harmful online content that could be fought more vigorously in a less complicated and excessive way than the bill the government envisions and wants to introduce. I do not think more Bureaucracy and changes to the criminal code, judicial tribunal and massive fines to citizens, among other ideas put forth in the bill, is necessarily the way to go. It also seems to be overly paternalistic. The government has a role in protecting its citizens, but this seems like an invasive micromanagement approach, with too much government involved online.

Groups designated as terrorist groups should have their posts and content removed online even if it does not incite violence. Anti-semitic content should be removed, including material that denies the holocaust. Fake news such as that related to covid-19 needs to be removed. Images or posts directed specifically at inciting violence, such as anti-semitic, islamophobic, Anti-Asian, calling for such groups' death or material related to terrorist attacks should be removed. Election misinformation online is a problem and should be taken seriously. Images of underage children, child exploitation should be removed. Harmful content comes in the form of images, but live-streaming violent and exploitive content is a problem. Live-streaming should be looked at as many social media are incorporating this into their platforms. Harmful audio should be looked at. If a terrorist group or a hate group posts audio calling for the death of a person or group of people, this should be taken down. These are some examples of my concerns about what I consider to be content that I am concerned about on social media.

Regarding what is harmful and hurtful, I think a clear distinction should be made with this bill between the two if it goes forward—inciting violence and hurtful feelings are not the same. Inciting violence online can constitute audio, speech, images that are threatening, intending to lead to physical injury and even death of someone or a group of people and can cause harm. Hurtful is not threatening but can make someone feel sad or lower their self-esteem. It is challenging to make the distinction between what is harmful and hurtful, and it has to be made cautiously and carefully regarding the internet. Especially since speech does not have to be text, it can be audio, images, and other things you may not have thought of as communication like memes, emojis and other emerging media.

I am disturbed by some of the comments that Heritage Minister Steven Guilbeault has said in the media about speech such as how the government thinks federal regulators should be given the authority to temporarily shut down websites or arrest people that say hurtful comments about politicians and civil servants.

I do not think a regulatory regime should target hurtful comments. Comments that make people sad or hurt their feelings but are not threatening with the intention of physical harm or someone's death. The same with hurtful audio or visual media. Blocking orders by a Digital Safety Commissioner for Social Media or a website because of what they consider hurtful, the content on it will make someone feel

sad or lower their self-esteem is wrong. Likewise, shutting down social media for the same reason should not occur. Guilbeault says blocking social media or websites is a last resort, comparing it to a nuclear bomb and saying it's an extreme measure, but it is a tool that could be used hypothetically. His comments are alarming. Based on his remarks, he also thinks that the online harms regulatory regime are needed because the internet and social media are undermining Canada's social cohesion. He told the press that world-renowned public servants leave politics because of what people say about them. It's rhetoric like this that scares me about this bill and makes me think that it could lead to Canadian's human rights being violated in an attempt to protect society, but it could also have negative consequences. Regulation of the internet is a slippery slope; if not done right, then the damage to Canadian society can be severe and maybe even permanent.

The government should not disregard people's lawful speech and expression, and the Charter of Rights and Freedoms should be respected, not eroded and stripped away in the process of attempting to "protect people" from social media and the internet by creating a new regulatory body to police the internet. If an individual is criticized or a civil servant and not threatened with violence, this is different than hurting someone's feelings.

It is useful for Canadians that the government is having a public consultation for Bill C-36 as not only industry "stakeholders" have the opportunity to voice their opinions. This is something that was missing from previous internet-related bills, and I think not having public consultation hurts public trust in the bill and the government's intentions. However, the public should have gotten a chance to give input before the bill was drafted. It would have added to the conversion of what is harmful and what is not. People could have had a chance to provide other solutions to the issues surrounding social media and the internet besides this concept of more Bureaucracy and harsh penalization that the government wants to impose as a solution.

Name: Laurence Price Address: Email:

s.19(1)

Date:	corrupting it. Just another Trudeau Pl July 29, 2021 3:48:31 PM
Subject:	Don't agree to having The Internet policed by an appointee of Government. No matter who you appoint they would be corrupted. I agree there are nasty things on the Internet but that is better than a Government HACK
To:	ICN / DCI (PCH)
From:	Bill Wagstaff the Access to Information

Sent from my iPhone

 From:
 Rod Reichheid

 To:
 ICN / DCI (PCH)

 Subject:
 Hate speech

 Date:
 July 29, 2021 8:06:37 PM

I don't know how Trudeau is going to define hate speech so for this reason I am against Trudeau and his regulations against Canadians saying what they want to especially when the truth hurts Trudeau and his scandals which HE hates to be known.

Sent from my iPad

From:	André Brunelle
To:	ICN / DCI (PCH)
Cc:	ANDRE BRUNELLE
Subject:	Disponibilité limitée des réseaux sociaux
Date:	July 29, 2021 3:43:56 PM

Pour les politiciens, il devrait être **interdit** d'utiliser les réseaux sociaux, qui pour certains, est une façon d'effectuer du lobbying gratuit et non sollicité auprès des électeurs. On a bien vu ce que pouvait donner l'abus politique des réseaux sociaux aux États-Unis avec l'usage qu'en faisait quotidiennement le président Trump. Il n'existe aucun contrôle sur la véracité des propos tenus et le dénigrement gratuit des adversaires politiques finissent par causer des émeutes comme celle du Capitol. Être en campagne électorale de manière perpétuelle, même quand on est au pouvoir, ça devient ahurissant à la longue pour les utilisateurs des réseaux sociaux.

André Brunelle

s.19(1)

Glen Smith
ICN / DCI (PCH)
The Government's proposed approach to address harmful content online
July 29, 2021 4:57:50 PM

There is some content put on the internet that is unequivocally illegal and harmful and should have no place for acceptance; and child pornography is probably the best example there is. I can even see an argument for identifying and removing overt and active terrorism plots (with proper legal thresholds to what that means).

However, I have grave concerns with the proposed categories of 'hate speech' and 'content that incites violence'.

Starting with the latter, what 'incites violence' is highly subjective, and therefore has a high likelihood of infringing on freedom of expression if the thresholds are not set very specifically and very high. For example, there is a large difference between someone saying 'Let's go meet at noon at a park and attack a person', and 'I hate that guy so much, I wish he was hit by a car'. The first implies action, the second does not. It raises the question of speach vs action; if the second scenario above inspired someone else to go and actually hit that person with a car, would the original author be guilty of inciting violence? They shouldn't be.

Just look at our neighbours to the south and the hugely divergent opinions on the January 6th Capitol Hill riots/assaults. Was ex-President Trump responsible for inciting violence via his tweets, even though there was no objective call to violence? The US is fully divided from 100% 'yes' to 100% no? Who's right? Who decides? Shouldn't the responsibility fall on those people who actually perpetrated the violence? It's entirely political, and political leaning should have no bearing on guilt or innocence; but that's what we're seeing down south. And that's what I do not want to see here.

Furthermore, even how the word 'violence' is used in the common vernacular is changing, where many people believe that speech that they don't like or that disapproves of some aspect of who they are is thought of as 'violence'. It's not. So once again, everything depends on exact definitions and thresholds, and this is something that is far too easy to get wrong, and the risks from getting it wrong are far too high. The word 'hate' is similar.

In terms of 'hate speech', this is an even more subjective category that I don't feel we should have laws about at all, let alone adding new ones. Is hatred based on intent or interpretation? Is it dependent upon the author, or the consumer? What is hateful to some is indifferent to others. Who decides? I have very large concerns with any person, company, or agency, with their own unique set of values, judging the content created by other bodies, with different sets of values, on what type of speech is offensive, hurtful, or hateful, or why this even matters. Almost everything will be offensive to someone; that doesn't mean it shouldn't be said. Everytime a limit is put on freedom of expression, it's only easier to put on more restrictions in the future.

And this is a very slippery slope, because people change, and those deciding what is or is not offensive or hateful now will not be the same as those in the future.

Having anybody make such subjective grey decisions and deciding what should or should not be said in public forum is dangerous, Orwellian, authoritative, impossible, and far too

susceptible to the ideologies of the majority .. .

 From:
 Stephanie E Perrin

 To:
 ICN / DCI (PCH)

 Subject:
 Two questions from the discussion of the technical paper

 Date:
 July 29, 2021 2:50:51 PM

Thanks for the technical briefing on this ambitious proposal. I have two immediate questions:

1. Do you anticipate any kind of judicial review?

2. Am I correct in assuming that content I put on a website, online subscriber journal, or blog, will not be covered? In the event that traffic migrates from social media platforms to these more old-fashioned methods, do you foresee enlarging the scope of the legislation?

Just a suggestion, it would be good to have a link to the paper and call for comments in the slide deck, for ease of distribution to other parties.

I would suggest that your concept of conflict of interest for the Commissioner is way too limited. You don't want a Commissioner from a targeted group, a civil liberties organization, or anyone with a horse in this race. Tall order, if you also want experience.

Yours truly,

Stephanie Perrin, President

Digital Discretion Inc.

 From:
 denis daviault

 To:
 ICN / DCI (PCH)

 Subject:
 Haine en ligne, contenu indésirable

 Date:
 July 29, 2021 3:17:42 PM

Merci de vous attaquer à ce fléau de notre démocratie. J'appuie le projet de loi

Envoyé de mon iPhone

From:	Toghrol, Ali
To:	ICN / DCI (PCH)
Subject:	Online Harms Legislation
Date:	July 29, 2021 3:00:36 PM
Importance:	Low

Unclassified

#### Good Afternoon,

I just participated in the teleconference and thank you for the information that you provided. I have two questions/suggestions. I believe it was mentioned that repeat offenders of Child Pornography and Terrorism postings will possibly be banned by their service providers? why would repeat offenders of Hate speech/propaganda not be subjected to the same rule. As you are aware Hate crimes, Radicalization and Terrorism are linked. Lastly although I applaud the 24hr window for platforms to remove posts I think that is a long time for something to remain and be shared online. Thank you again.

AT

A/Sgt. Ali Toghrol Ottawa Police Service Hate & Bias Crime Unit Office: 613.236.1222, ext. 5453 Fax: 613.760.8075 Mailing address: P.O. Box 9634, Station T, Ottawa, ON K1G 6H5 Toghrola@ottawapolice.ca

 From:
 colan mitchell
 INE /

 To:
 ICN / DCI (PCH)

 Subject:
 The Government's proposed approach to address harmful content online

 Date:
 July 29, 2021 12:17:06 PM

Canada already has laws that cover hate speech, promoting violence, and illegal activity. The country does not need another layer of Liberal bureaucracy.

Colan Mitchell



## **Policy Recommendations on Online Hate**

Document communiqué en vertu de

Horrific events of the last century have demonstrated that words matter. Hateful and intentionally deceptive words can lead directly to violent actions targeting individuals and groups. We must be vigilant in identifying and exposing online hate and purposeful disinformation that has the potential to incite violence or promote injustice against ethnocultural, racial, religious and other identifiable groups. The rapid proliferation of social media and online communications has made this task more important than ever.

The task of combating online hate and disinformation is even more urgent in the context of the Covid-19 pandemic. Numerous studies have pointed to the role of state-sponsored disinformation campaigns about the pandemic by regimes adversarial to Canada and democratic values, such as Russia.

The Ukrainian Canadian community has experienced increasing volumes of targeted online operations in the form of disinformation. This information warfare – as part of Russia's war on Ukraine – is intended to undermine our community by distorting historical truth, sowing division, and weakening support for democratic institutions.

These campaigns reach far beyond the Ukrainian community. The 2019 Annual Report for the National Security and Intelligence Committee of Parliamentarians found that: "The Russian Federation engages in foreign interference activities across Canada's political system with the objective of influencing government decision-making and swaying public opinion. [...] The nature and extent of Russia's foreign interference threat is significant as these activities form a key component of the broader national security threat posed by Russia."

Multiple think-tanks in Canada, the US and the EU have established that these malign influence

#### **OUR RECOMMENDATIONS**

- Counter online hate and disinformation spread by adversarial regimes
- Remove RT, Sputnik and other Russian state broadcasters from Canadian airwaves
- Strengthen cyber security
- Hold social media platforms to account

## Document communiqué en vertu de la Loi sur l'accès à l'information. Policy Recommendations on Online Hate

operations are not specific to one platform, actor or targeted group. Information warfare is a global problem; its intent is to sow division within and between western democracies and alliances, subvert international institutions, and erode public trust and social cohesion. The UCC will continue to work with both Ukrainian and Canadian institutions, along with think tanks and other organizations working to fight disinformation, and to identify fake news and propaganda.



The Russian government carries out its media influence operations in myriad ways, including through state-controlled or state-sponsored media outlets that are freely available in Canada, both in traditional television and in online formats. Social media platforms, internet companies and the Canadian Radio-television and Telecommunications Commission have proven either unable or unwilling to counter these threats.

The rapid proliferation of online hate and targeted disinformation needs to be addressed by today's policy-makers

## Recommendations

Counter online hate and disinformation spread by adversarial regimes The UCC believes that the issues of foreign state interference and disinformation and the issue of online hate are inextricably linked. The UCC is part of a broad coalition, the Canadian Coalition to End Online Hate, which submitted recommendations to the Government of Canada in May 2020.

Among the recommendations of the Coalition was for the Government to "review the role of, and develop a strategy for, combating online hate that is sponsored or supported by authoritarian governments, state broadcasters of authoritarian regimes and foreign organizations."

The Government of Canada has introduced legislation, Bill C-36, the aim of which is "to better protect Canadians from hate speech and online harms."

The UCC calls on the Government of Canada, in proposed legislation combatting online hate, to dedicate due focus to the role played in the dissemination of online hate, of regimes and governments adversarial to Canada and democratic values.

# Document communiqué en vertu de la Loi sur l'accès à l'information. Policy Recommendations on Online Hate

Remove RT, Sputnik and other Russian state broadcasters from Canadian airwaves

Strengthen cyber security

Hold social media platforms to account RT Sputnik and other Russian state television and online propaganda are serious threats to the integrity of impartial news programming in Canada. In 2020, Canada's NATO ally Latvia banned the channel RT. Latvia's regulator, Electronic Mass Media Council (NEPLP), found that RT is under the "effective control" of Dimitry Kiselev, who is under both EU and Canadian sanctions. NATO ally Lithuania followed suit a few months later, and banned RT from broadcasting in Lithuania. The CRTC has failed to take similar action and RT continues to broadcast in Canada.

The UCC calls on Canada to remove RT, Sputnik and other Russian state broadcasters from Canadian airwaves and online space.

A July 2021 report by the Communications Security Establishment of Canada found that, "From 2015 to 2020, we judge that the vast majority of cyber threat activity affecting democratic processes can be attributed to state-sponsored cyber threat actors. These actors target democratic processes in pursuit of their strategic objectives (i.e., political, economic, and geopolitical). Russia, China, and Iran are very likely responsible for most of the foreign state sponsored cyber threat activity against democratic processes worldwide."

The UCC calls on the Government of Canada to dedicate appropriate resources to countering cyber threat activity carried out by state-sponsored cyber threat actors and to respond strongly to cyber attacks on Canadian communications infrastructure.

The UCC supports the development of legislative measures that would hold social media platforms to account for failing to remove hate speech and purposeful disinformation from their platforms.

The UCC calls on the Government of Canada to work swiftly to eliminate online hate from social media networks, including Russian disinformation campaigns that knowingly promulgate hatred against Ukraine and Ukrainians.

 From:
 Rick Pelletier

 To:
 ICN / DCI (PCH)

 Subject:
 This "harmful content" proposal is nothing short of ridiculous

 Date:
 September 22, 2021 4:32:11 PM

The proposals as outlined will do nothing useful against actual harmful content online, while simultaneously hamstringing and crippling Canadian companies and companies doing business in Canada.

The very concept of the proposals is so far removed from reality that I laughed before realizing that someone, somewhere, actually thought this EXEMPLARY stupidity was a good idea.

Signed,

A Canadian systems administrator and citizen

# Rebecca De Lachevrotiere Lalonde

From: Sent: To: Subject: Nathan RicciutiSeptember 25, 2021 11:18 PMICN / DCI (PCH)NO to Canada's harmful content proposal

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

l urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Nathan Ricciuti

handarian esta dalappo anti-sentra la creativa en la 2010 failorna han 2010 mente alconal dalariana dal 1010 mente del anti-material

# Rebecca De Lachevrotiere Lalonde

From: Sent: To: Subject: Dragica Durajlija September 25, 2021 11:14 PM ICN / DCI (PCH) NO to Canada's harmful content proposal

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

l urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Dragica Durajlija

tenstanten este stettaj son sonata la en gran de Sen Difformel en 2000 mentenkonstetta en antiere dire treeste de antieren antes s

### Rebecca De Lachevrotiere Lalonde

From: Sent: To: Subject: David McCauley -September 25, 2021 11:14 PM ICN / DCI (PCH) s.19(1) NO to Canada's harmful content proposal

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, David McCauley

#### Rebecca De Lachevrotiere Lalonde

From: Sent: To: Subject: Dave Haywood September 25, 2021 11:12 PM ICN / DCI (PCH) s.19(1) NO to Canada's harmful content proposal

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Dave Haywood

### Rebecca De Lachevrotiere Lalonde

From:	
Sent:	
To:	
Subject:	

Sandra Jeanneret September 25, 2021 11:08 PM ICN / DCI (PCH) s.19(1) NO to Canada's harmful content proposal

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Sandra Jeanneret

teneral conception of the second second

### Rebecca De Lachevrotiere Lalonde

From: Sent: To: Subject: Trish Denise September 25, 2021 10:56 PM ICN / DCI (PCH) NO to Canada's harmful content proposal

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Trish Denise

# Rebecca De Lachevrotiere Lalonde

From: Sent: To: Subject: Howard Bittner September 25, 2021 10:52 PM ICN / DCI (PCH) NO to Canada's harmful content proposal

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

l urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Howard Bittner

### Rebecca De Lachevrotiere Lalonde

From: Sent: To: Subject: Rita Coughlin September 25, 2021 10:50 PM ICN / DCI (PCH) NO to Canada's harmful content proposal

s.19(1)

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Rita Coughlin

handarian esta dalappo anti-sentra la creativa e de la Pathornal cargarangen kasha anti-tarangen la creativa de anti-tarangen est

## Rebecca De Lachevrotiere Lalonde

From: Sent: To: Subject: Beverley Baltimore September 25, 2021 10:46 PM ICN / DCI (PCH) S.19(1) NO to Canada's harmful content proposal

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Beverley Baltimore

teneral en este statut per a sentar la crea que com de la fattarina han gana manda esta com ta comunato de strectiva de anataricado est

#### Rebecca De Lachevrotiere Lalonde

From:
Sent:
To:
Subject:

Andy Akey September 25, 2021 10:44 PM ICN / DCI (PCH) NO to Canada's harmful content proposal

s.19(1)

As a concerned person in Canada, I urge you to abandon the draft proposals for our Internet outlined in your consultation paper on harmful content online. If implemented, these measures will lead directly to the removal of many lawful posts in Canada, including important forms of protest and personal expression.

In the offline world, restrictions on our freedom of expression are tightly limited, and surveillance by law enforcement requires approval of a court. By deputizing online platforms to proactively surveil, police, and remove our content, your proposal reverses this healthy offline balance. Online platforms afraid of your punitive legislation will not carefully weigh our posts, and many posts that would not be found illegal offline will certainly be removed by platforms and reported to law enforcement.

I strongly oppose the disproportionate and poorly conceived measures proposed in your consultation, including mandatory 24-hour takedown windows, reporting of removed posts to law enforcement, forcing platforms to proactively surveil their users' posts, and any plans for blocking of websites in Canada.

These proposals are very likely to be used to police and harass already marginalized people on the Internet, not to protect and empower them.

I urge you to work with academic experts, civil society, and online platforms themselves on developing a more thoughtful, measured approach to addressing illegal and harmful content online.

Kind regards, Andy Akey

 
 From:
 Paul Deegan

 To:
 ICN / DCI (PCH)

 Subject:
 Submission from News Media Canada

 Date:
 September 16, 2021 5:02:35 PM

 Attachments:
 NMCOnlineHarmsSubmission.pdf PastedGraphic-1.tiff

Attached is News Media Canada's submission to the online harms consultation.

Best regards,

Paul

Paul Deegan President and Chief Executive Officer News Media Canada | Médias d'Info Canada

37 Front Street East, Suite 200 Toronto, Ontario M5E 1B3 pdeegan@newsmediacanada.ca 647-992-5522 Document communiqué en vertu de <u>News Media Canada</u> la Loi sur l'accès à l'information <u>Médias d'Info Canada Document released pursuant to</u> the Access to Information Act

September 16, 2021

Digital Citizen Initiative Department of Canadian Heritage 25 Eddy St Gatineau QC K1A 055

VIA EMAIL: pch.icn-dci.pch@canada.ca

To whom it may concern:

News Media Canada, which represents Canada's news publishers who employ 3000 journalists from coast to coast to coast, believes that free speech, journalistic freedom, and a strong, healthy, commercially viable, and fiercely independent media ecosystem are all vital to our democracy.

Canadians rely on their newspapers and news media to be their trusted sources of information, helping them make informed choices and holding people and institutions, including governments and corporations, accountable.

We welcome the opportunity to participate in this Consultation, and we appreciate the Government's commitment to taking meaningful action to combat hate speech and other kinds of harmful content online, while ensuring that freedom of expression and free debate are recognized, preserved, and protected.

We are among the country's leading defenders of freedom of speech. At the same time, as employers, we strive to provide a safe, healthy, and inclusive work environment for our journalists. As businesses who supply news and analysis, we also strive to protect our customers: the public who read our news and engage with us and their fellow readers. We listen to our customers. We take our responsibilities to them and the broader public seriously. We try to build a better common future for all. And we are accountable for both our actions and inaction.

As a business, the news publishing industry remains under threat from the unregulated and unchecked social media and other online communication service providers. At the same, our journalists—including female and BIPOC journalists—and our customers face online harm.

Across the globe, journalists face physical, judicial, and online harm. In addition to harassment from individuals, journalists face sophisticated defamation campaigns to discredit and silence them. These threats, and their potential impact on journalistic freedom of expression, have detrimental implications for society at large.



News Media Canada Médias d'Info Canada Document communiqué en vertu de la Lol sur l'accès à l'information Document released pursuant to the Access to Information Act

The findings of a <u>survey</u> conducted by the United Nations Educational, Scientific and Cultural Organization and the International Center for Journalists, about online violence against women journalists are alarming:

- 73% of women respondents said they had experienced online violence.
- 20% said they had been attacked or abused offline in incidents seeded online.
- 41% said they had been the targets of online attacks that appeared to be linked to orchestrated disinformation campaigns.

The impact on this violence on mental health is sobering:

- .38% missed work.
- 11% quit their jobs.
- 2% abandoned journalism altogether.

It also impacts journalistic practices and audience engagement:

- 30% self-censor on social media.
- 20% only 'broadcast' and avoid all interaction.
- More troubling, 10% avoid pursuing particular stories.

Like news publishers, online platforms curate content. They reap all the benefits of being a publisher, albeit on much more commercially favourable terms, yet they do not have the same responsibilities, and are not held accountable in the many ways that news publishers are in Canada. Indeed, they have allowed fake news and disinformation to proliferate around the globe.

Big Tech has a societal obligation to moderate these activities, just as any news publisher does. However, Section 230 of the Communications Decency Act exempts them from liability over hosting user-generated content and from liability when they choose to remove that content. Global companies operating in Canada are subject to Canadian law and should conduct themselves accordingly.

As advertisers know, these firms have enormous and extremely sophisticated technical prowess. Why then have they failed in their duty as content moderators and allowed harmful content targeted at journalists to be amplified on their platforms?

As a matter of principle, our journalists should be afforded the same protections in the online world as they are in the offline world. Accordingly, we recommend that the Government of



News Media Conoco Médias d'Infa Conoco Document communiqué en vertu de la Loi sur l'accès à l'information Document released pursuant to the Access to Information Act

Canada explicitly recognize online threats to journalists directly into the Act. Journalists should be afforded "exceptional recourse" to online threats.

News Media Canada submits online platforms should:

- Act upon reports of harassment from news publishers and journalists within 24 hours.
- Invest in technology to detect online hate against journalists.
- Detail online harm against journalists in their transparency reports.
- Be held accountable through Canada's libel, defamation, and hate laws, just as Canada's news publishers are.
- Face economic penalties when they fail to comply with Canadian laws.
- Make it hard for internet trolls to 'profit' from the monetization of content that harms journalists.

This is not about limiting democratic expression; it is about protecting it and its most precious guardians; Journalists. And it is about ensuring *all* publishers, including internet intermediaries, are held accountable for harmful content by being transparent in their policies, expeditious and robust in applying those policies and in meeting obligations to customers, and compliant in meeting Canadian legal obligations.

Sincerely,

Paul Deegan President and Chief Executive Officer