

Commissariat  
à la protection de  
la vie privée du  
CanadaOffice of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
	2 + attachments

**NOTE D'INFORMATION****BRIEFING NOTE**

## National Security Consultations Timelines and Outline

**OBJET / PURPOSE:** To inform you of the way forward for the Public Safety consultations on National Security.

**CONTEXTE / BACKGROUND:**

Further to a briefing note prepared for you on this matter, and subsequent meetings, you will find attached an outline document which will form the basis of the Office's submission to the above-referenced consultations. The outline follows the structure of the consultation backgrounder "Our Security, Our Rights: National Security Green Paper, 2016"<sup>1</sup> and includes placeholders for what will eventually become the submission text. It includes endnote references which point to pre-existing material which can be drawn upon.

You will receive portions of proposed text for your review prior to each meeting, the dates of which are already in your calendar.

For the purposes of translation, and in order to ensure we meet Public Safety's submission deadline of December 1, we propose limiting ourselves to a maximum of 15 pages.

**CONSULTATIONS:** Legal Services (Julia Barss, Michael Sims, Sarah Speevak)

**RELATED DOCUMENTS / DOCUMENTS CONNEXES:**

- Submission on National Security Consultations (Public Safety Canada) 7777-6-164260
- Public Safety National Security consultation backgrounder - Our Security, Our Rights 7777-6-164257
- Briefing Note - participation in Public Safety's consultations on national security - September 2016 7777-6-162822

**DISTRIBUTION:** Commissioner, LSPRTA

**APPROBATION / APPROVAL:**

Rédigé par / Prepared by	Date	Revisions
Leslie Fournier-Dupelle	September 22, 2016	

<sup>1</sup> Available online at <http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx> and in Officium at 7777-6-164257

Approuvé par / Approved by Date

*B Bucknell* 23/9/16

Barbara Bucknell  
Directrice, Politiques et recherche / Director, Policy and Research

Approuvé par – Approuvé par Date

*Patricia Kosseim* 23/9/16

Patricia Kosseim  
Avocate générale principale et Directrice générale / Senior General Counsel

Approuvé par / Approved by Date

- Je suis satisfait des mesures proposées. / I agree with the proposed recommendation(s).
- Je ne suis pas satisfait de ces recommandations pour les raisons suivantes. / I do not agree with the proposed recommendation(s) for the following reason(s):

Commentaires ou des instructions supplémentaires / Additional Comments or Instructions:

I would not assume that the structure & content within the 8 chapters or issues will be as proposed: that should be discussed & agreed upon at the meetings I have scheduled.  
Glad to discuss what that means for your prep work & whether the meetings are too late to "land" by Dec. 1.

Daniel Therrien  
Le commissaire à la protection de la vie privée / Privacy Commissioner

In addition, I may want to "land" before Dec. 1 so as to be available for the media upon publication and, ideally, also attend APPA.

*[Signature]*  
23/9/16

Commissariat  
à la protection de  
la vie privée du  
Canada

Office of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
Unclassified	10 + attachment

---



---

## NOTE D'INFORMATION

## BRIEFING NOTE

---



---

### Online Reputation – Summary of Submissions

**PURPOSE:** To provide a summary of the submissions received in response to the OPC's call for essays on online reputation and identify solutions to be explored further.

**OVERVIEW:** The OPC received a total of 25 submissions – 24 external and one from an OPC employee writing as a private individual. OPC's stakeholder community was well represented through a balance<sup>1</sup> of industry, academics, civil society, lawyers and the general public.

Submissions presented a broad range of solutions from standardized takedown request forms and procedures to enhanced powers for the OPC. The Right To Be Forgotten (RTBF) was referenced in over half the submissions, with most against the European model of RTBF but many in favour of the idea that individuals should have a right to have their personal information deleted in specific circumstances. Details of the submissions follow.

#### BACKGROUND:

In January 2016, the discussion paper entitled "Online Reputation – What are they saying about me?" was posted to the OPC website<sup>2</sup>. The paper aims to advance public debate on online reputation and privacy, one of the OPC's privacy priorities, with a longer-term goal of better positioning the OPC to inform Parliament of a variety of solutions for addressing issues related to online reputation and developing a policy position on this issue.

The discussion paper invited interested parties to propose new and innovative ways to protect reputational privacy and to help bring clearer definition to the roles and responsibilities of the various players that could implement them.

---

<sup>1</sup> Breakdown of submissions: Academics – 4; Civil Society – 3; Industry – 7; Media – 3, Lawyers – 5; Individuals (Comment Form Input) – 2; OPC employees – 1

<sup>2</sup> [https://www.priv.gc.ca/information/research-recherche/2016/or\\_201601\\_e.asp](https://www.priv.gc.ca/information/research-recherche/2016/or_201601_e.asp)

## SUMMARY OF SUBMISSIONS:

A grid of comments received from stakeholders is shown at Appendix A to this note. What follows is a narrative summary of the submissions, organized by discussion questions posed in the reputation paper.

**We have highlighted some potential gaps in protections between the online and offline worlds. What other gaps exist?**

Two submissions addressed what they identified as the inaccessibility of legal recourse to individuals. Avner Levin underlined the need for innovative and affordable solutions that will allow individuals to exercise better control over their reputations and personal information without incurring high legal costs. ITAC called on the federal government to provide individuals with efficient means of redress through existing legal mechanisms while avoiding the time, effort and expense currently being faced.

Site architecture was mentioned as a significant factor hindering individuals, particularly young people, from having meaningful control over their personal information and reputation. The Steeves/Bailey submission states “networked media create a ‘perfect storm’ in which architectures incent disclosure of information by young people that is in turn used in commercial advertising and other marketing material premised on narrow stereotypes. Young people reproduce these stereotypes in order to attract “likes”, but their success or their failure opens them up to conflict with others who monitor and judge their self-representations.” In their view, consent does not work in this environment because young people have no choice but to accept the terms of service and participate because networked technologies are embedded in their lives. Other submissions mentioned the difficulties in understanding privacy settings and procedures for requesting takedown of content, which vary across different sites and services. Solutions were proposed to address these issues, as outlined below.

Finally, the lack of order making power was seen as limiting the OPC’s effectiveness in addressing online reputation problems. Slane/Langlois and Avner Levin proposed that the OPC advocate for stronger enforcement powers, including the power to levy AMPs.

**What practical, technical, policy or legal solutions should be considered to mitigate online reputational risks?**

Limiting collection of personal information : In the context of site architecture, the Steeves/Bailey submission offers practical solutions which recognize that participation in networked spaces is not optional for young people. It is for this reason that Steeves/Bailey state “approaches focused solely on requiring further disclosure of corporate practices are unlikely to affect any real change.” They propose that sites create easy ways for users to opt out of information collection, and include some options for communication that will not be monitored. As well, they encouraged the OPC to use existing powers, such as section 5(3) to limit practices that implicate young people’s personal information. For example, they suggested that the flow of information captured by educational software be strictly regulated or prohibited.

Privacy Settings & Notice: BC FIPA called on architects of information-sharing platforms to encourage privacy protection, and “give individuals a better sense of the privacy protections they may choose to give up.” BC FIPA also communicated a need for sites to implement standardized privacy settings to create less confusion for users. Also suggested were stronger default settings and requiring explicit consent for making privacy settings more open.

Standardized Takedown Procedures: BC FIPA called for better transparency and a standardized process for removing or obscuring personal information across platforms. Similarly, Avner Levin proposed a standardized form across all online services for requesting that personal information be removed or corrected.

Education: Many submissions recommended strengthening education initiatives around digital ethics and individual responsibility in posting personal information online. ITAC proposed that “cyber hygiene” (digital security and digital literacy) be a core component of school curricula. The OPC was encouraged to continue its public education role. TELUS advocated for collaboration between government and industry to develop and share educational resources. Media Smarts suggested that:

- Teachers be provided with professional development on digital issues;
- Parents be given accurate information and given practical tools for discussing digital issues with their children;
- Further research be conducted into youth norms and attitudes on privacy; and
- Digital literacy be embedded in the K-12 curriculum across Canada.

7. Mention was made of reputation management companies and their usefulness in helping individuals find and correct or delete misleading information. It was suggested that the reputation management companies should continuously patrol big data and report their findings to individuals through a simple interface.

To tackle the problem of protecting online reputation across multiple jurisdictions, ITAC proposed that Canada pursue the creation of Mutual Legal Assistance Treaties to expedite legal processes. Slane/Langlois also suggested that OPC strengthen coordination with provincial consumer protection enforcement to address the problem of revenge porn sites.

Slane/Langlois also proposed that PIPEDA be amended to make liable businesses that encourage and profit from users posting sensitive personal information, like revenge porn sites. As well, they suggest the OPC should be empowered to prohibit those businesses from carrying on with those practices and to impose administrative monetary penalties. Steeves/Bailey proposed that the OPC use existing powers, such as s. 5(3) to limit corporate collection, aggregation and monitoring of young people’s data. As well, personal information of young people should not be kept indefinitely.

BC FIPA referenced a suggestion by academics<sup>3</sup> that individuals have a legislated right to obscurity, particularly for information that might be embarrassing but “is not damaging enough to warrant the full force of robust privacy and confidentiality protections.”

---

<sup>3</sup> Hartzog and Stutsman

Can the right to be forgotten find application in the Canadian context and, if so, how?

## European model

The “right to be forgotten” (RTBF) was by far the most popular topic in the submissions, referenced by 14 stakeholders either exclusively or in part. Most<sup>4</sup> submissions, including the 3 submitted by media organizations, were opposed to the European model of the RTBF. Reasons included:

- the responsibility of balancing interests should not be transferred from the Courts to multinational corporations;
- lack of transparency and oversight; and
- too onerous for search engines.

Google suggested that any RTBF framework to be considered in Canada must have transparency, accountability and recourse mechanisms. It cited the difficulties it faced in terms of value judgments, with the incentive being skewed toward removal due to liability issues. BC FIPA suggested that, whenever possible, the content creators or hosts should be notified and given the opportunity to dispute any removal or obscurity requests based on their own rights and interests or a public interest, and sufficient time should be taken to consider the legitimacy of the requests. Both Google and the BC FIPA suggested that the RTBF would pose a barrier to market entry for new search engines because of the resource burden.

## Charter issues

The three media organizations see the RTBF as a threat to free expression and press freedom. In their opinion, the RTBF is a European principle that is inconsistent with Canadian values, and risks giving individuals, particularly the wealthy and powerful, the right to rewrite history. It also makes it more difficult for journalists to reach the public.

Many submissions cited Charter issues with the RTBF. David Fraser stated “we are not only concerned with a search engine operator’s constitutionally protected right to freedom of expression, but the right of every Canadian to get access to relevant content on the internet via the use of Google’s search engine. This also limits Canadian media outlets’ constitutionally protected right to disseminate its expressive content on the internet.” The Gratton/Polonetsky submission echoes this point and suggests that the RTBF might strike an appropriate balance between freedom of expression and privacy if it were limited to “intrinsically intimate information which creates a risk of harm.” (Slane/Langlois also propose a very limited application of RTBF, without mentioning the Charter, as discussed further in this note.)

---

<sup>4</sup> Avner Levin alone wrote in support of the European model. While acknowledging problems with the model, he said “these critiques pale in comparison with the significance of offering millions of users a cheap and easy remedial tool.”

Mr. Fraser, Ms. Gratton and Mr. Polonetsky cite numerous reasons in support their position including:

- Vagueness of criteria for removal of content;
- Lack of procedural fairness;
- Search engines are biased toward removal of content to limit their liability, thus the balancing of interests is not impartial;
- If RTBF were created under or read into PIPEDA, PIPEDA would outlaw the collection/use and disclosure of personal information for many legitimate expressive purposes related to seeking information and knowledge; and
- PIPEDA does not include any mechanisms for balancing freedom of expression with privacy interests.

Mr. Fraser also argues that RTBF would violate the separation of powers guaranteed under the Charter. Citing *General Motors of Canada Ltd. V. City National Leasing*<sup>5</sup>, Mr. Fraser claims that the RTBF is not a valid exercise of the general Trade and Commerce power because it does not regulate the economy or trade as a whole but as a single commodity - the operation of search engines.

Other submissions suggested that the RTBF would infringe on a broad range of interests, not just freedom of expression but also openness of the judicial process, and the public's right to know. The CMA's submission stated that the RTBF would be contrary to public policy objectives because history is being rewritten or obliterated, search results are incomplete or less relevant. The BC FIPA suggested that the RTBF will create inequality between those who know how to look for information and those who do not.

### Is RTBF required in Canada?

Some felt that solutions already exist to the problems RTBF is meant to address. These solutions include defamation law, privacy torts, website takedown policies, and PIPEDA. For example, the CMA argued that PIPEDA already provides a framework for management of personal information through the provision of obligations on organizations that collect, use and disclose personal information as well as rights for individuals. Obligations include obtaining informed consent, limiting collection to that necessary for the purposes, collecting by fair and lawful means, retaining for only as long as is necessary to fulfill the purposes, and ensuring information is accurate, complete and up-to-date. Individuals have the right of access, correction and withdrawing consent.

The Gratton/Polonetsky submission presented similar arguments and suggested that laws which restrict availability or use of personal information were worth exploring as a solution in some circumstances. The examples listed included clean slate laws, such as credit reporting and juvenile criminal law, which limit retention, as well as employment laws that prohibit employers from asking for social media passwords.

---

<sup>5</sup> *General Motors of Canada Ltd. V. City National Leasing*, (1989) 1 SCR 641, 1989 CanLii 133

## **Is there a RTBF in PIPEDA?**

Some stated that there is no legislative basis for RTBF. David Fraser argued that search engines' search function is not covered under PIPEDA because there is no commercial activity – it's free for individuals to search and free for content providers to be indexed. He also thinks that search engines are engaged in journalistic or literary activity when they are providing individuals with links to news media content and media producers with access to readers. On the flip side, Christopher Berzins posited that there may be a reasonable basis for a complaint under PIPEDA requesting removal of personal information from Google because Google is engaged in commercial activity, it does not obtain consent for the collection, use or disclosure of personal information in search results, and no PIPEDA exemptions apply. Avner Levin suggested that the OPC should make a finding in a RTBF complaint and, if necessary, ask the Court to confirm that the RTBF exists in Canada.

## **Should there be special measures for vulnerable groups?**

Women were identified by multiple submissions as being particularly vulnerable to reputational harm online. The Slane/Langlois submission focussed on revenge porn sites and suggested that businesses which specifically encourage and profit from users posting sensitive and damaging information about others should be liable under PIPEDA. They also suggest that PIPEDA should be strengthened to expressly allow for prosecution of such businesses.

Education was repeatedly suggested as a way of reducing the reputational harm faced by women, girls and other vulnerable groups, such as minorities, First Nations, LBGTQ, high risk youth and seniors. Specifically, it was suggested that such individuals should be made aware of their rights in online spaces and empowered to build communities where their rights are respected. Educational measures were also suggested to combat negative attitudes about vulnerable groups and to teach the importance of privacy. TELUS recommended that the OPC make a special effort to reach out to organizations that work with vulnerable individuals and marginalized communities in order to gain a better understanding of their specific needs and how to address them.

Jonathan Obar suggested the development of policies to protect communities that are more likely to be the subject of big data-driven discrimination. BC FIPA suggested that improvements be made to human rights and employment laws to better protect disadvantaged groups and individuals who suffer as a result of damage to their online reputation.

## **Who are the key players and what are their responsibilities?**

A couple of submissions cautioned against putting all of the responsibility for protecting reputation on individuals. Steeves/Bailey stated that "policymakers should pay more attention to corporate practices and policies that compromise individuals' ability to negotiate (online) privacy." Other disagreed. For example, TELUS felt that individuals must play a key role in taking responsibility for online privacy and reputation; understand the online products and services we use; and the implications of sharing information about us and others. TELUS also stated that it is the responsibility of industry, government, law



s.21(1)(a)

s.23

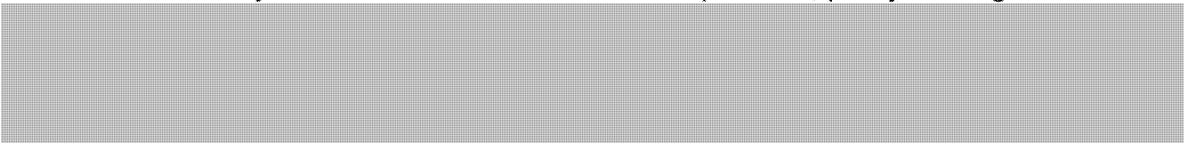
enforcement, education and topic experts to collaborate on educating Canadians.

The Family Online Safety Institute stated that companies have a responsibility to create robust technical settings to increase user control, and promote their usage to lessen the risk of reputational harm. Companies should also provide educational messaging to help users determine how much and with whom they want to share their information. Parents should encourage their children to use online privacy tools.

The OPC was seen as having a strong education and research role, as mentioned earlier. As well, Avner Levin suggested that the OPC should advocate for the creation of more regulatory-driven/technologically enabled solutions that are low-cost, easy to use and alleviate the need for regulator intervention.

### **PRELIMINARY ANALYSIS AND ISSUES FOR DISCUSSION:**

The possibility of a RTBF in Canada is clearly of concern to many of the OPC's stakeholders. According to many of the submissions received, implementing the European model of RTBF may not be desirable for a number of practical, policy and legal reasons.



The RTBF aside, stakeholders proposed many solutions aimed at enhancing individuals' understanding of the online world, enhancing individuals' ability to exercise practical control over online personal information, and enhancing oversight and accountability of organizations.

Some of the proposed solutions are non-controversial and present an opportunity for the OPC to either enhance work already being undertaken or to explore taking action in the future. Specifically:

1. Collaborate with industry to develop and share educational materials<sup>1</sup>;
2. Launch a public awareness campaign to encourage the public to think twice before they post<sup>2</sup>;
3. Conduct in-personal seminars and provide educational materials through various media;<sup>3</sup>
4. Continue to target teachers and parents on digital issues affecting children and youth;<sup>4</sup>
5. Support education efforts by healthcare providers, public health authorities, youth advocates and counsellors, community groups and media producers;<sup>5</sup>
6. Promote education on fostering empathy in online contexts;<sup>6</sup>
7. Reach out to organizations that work with vulnerable individuals and marginalized communities to customize education to those specific audiences;<sup>7</sup>
8. Help teach children and youth to use existing privacy tools and settings to help them manage their reputation;<sup>8</sup>

9. Conduct or support research into youth norms and attitudes on privacy;<sup>6</sup> and online reputation's effects on the online and offline lives of individuals.<sup>9</sup>

Some of these suggested initiatives in relation to youth and digital education are already being pursued in the context of an FPT working group led by the OPC that intends to collaborate on efforts to enhance privacy education to youth, as well as the OPC's participation on the International Conference of Data Protection and Privacy Commissioners Digital Education Working Group.

Some other proposed solutions should be discussed internally to identify risks and benefits, as well as a role for OPC and the risks and benefits of the proposed solution. These are listed below:

1. Standardize takedown request forms and procedures across online services<sup>10 11</sup> - These proposed solutions could be explored in the context of our work on consent and promoting industry codes of practice;
2. Enhance privacy controls<sup>12</sup> by promoting stronger defaults, standardization across platforms, and obtaining consent before changing privacy settings for existing users (this area could be a candidate for a code of practice);
3. Encourage technology companies to look to industry best practices to create robust technical settings to increase user control, and promote the use of existing tools by individuals;<sup>13</sup> (again, a possible are for a code of practice)
4. Prohibit the c/u/d of personal information in very limited circumstances where reputational harm is particularly egregious – for example, revenge websites;<sup>14</sup>
5. Give the OPC order making powers and the power to levy AMPs against online businesses that specifically promote and encourage users to post damaging content;
6. Promote the concept of practical obscurity<sup>15</sup> (this could be explored in the context of administrative tribunals that fall under the Privacy Act);
7. Explore stricter retention and deletion policies for young people's data<sup>16</sup>;
8. Using existing powers to limit corporate collection, aggregation and monitoring of young people's data<sup>17</sup> (this would involve expanding the approach we already take with children's personal information to an older age group.);
9. Collaborate with consumer protection regulators to address the problem of revenge websites;<sup>18</sup>
10. Examine Quebec defamation law with a view to adopting its higher protections;<sup>19</sup>
11. Help enhance laws that restrict the availability and use of personal information, such as clean slate laws and employment laws that prohibit the use of social media information during the hiring process;<sup>20</sup> and
12. Help enhance human rights law and employment standards with a view to improvements to better protect disadvantaged groups.<sup>21</sup>

It is suggested that an internal discussion take place to review the proposed solutions and come to a consensus on their viability as a preliminary step in drafting the OPC position paper on reputational privacy and recourse mechanisms.

---

<sup>6</sup> MediaSmarts and FOSI

A proposed outline for the position paper can be found at Appendix B

**APPENDICES:**

APPENDIX A : Online Reputation Submissions – summary grid (officium 7777-6-145879)

APPENDIX B: Draft outline for position paper (officium 7777-6-148985)

**DISTRIBUTION:** Commissioner, LSPRTA, Brent Homan, Anne-Marie Hayden

**APPROBATION / APPROVAL:**

Rédigé par / Prepared by	Date	Revisions
Kasia Krzymien and Melissa Goncalves	May 31, 2016	June 3, 2016 June 9, 2016 June 14, 2016
<p><b>Approuvé par / Approved by</b> <span style="float: right;"><b>Date</b></span></p> <p style="text-align: center;"><i>B Bucknell (w minor changes) 16/6/16</i></p> <p>Barbara Bucknell <i>Directrice, Politiques et recherche / Director, Policy and Research</i></p>		
<p><b>Approved by – Approuvé par</b> <span style="float: right;"><b>Date</b></span></p> <p style="text-align: center;"><i>Patricia Kosseim 23/6/16</i></p> <p>Patricia Kosseim <i>Avocate générale principale et Directrice générale / Senior General Counsel</i></p>		

Approuvé par / Approved by	Date
<input type="checkbox"/> Je suis satisfait des mesures proposées. / I agree with the proposed recommendation(s). <input type="checkbox"/> Je ne suis pas satisfait de ces recommandations pour les raisons suivantes. / I do not agree with the proposed recommendation(s) for the following reason(s):	
Commentaires ou des instructions supplémentaires / Additional Comments or Instructions:	
Daniel Therrien <i>Le commissaire à la protection de la vie privée / Privacy Commissioner</i>	

- 1 TELUS
- 2 ITAC
- 3 TELUS
- 4 MediaSmarts
- 5 MediaSmarts
- 6 MediaSmarts
- 7 TELUS
- 8 FOSI
- 9 BC FIPA
- 10 Levin, Steeves and Bailey,
- 11 Gratton and Polonetsky
- 12 BC FIPA
- 13 FOSI
- 14 Slane and Langlois
- 15 BC FIPA
- 16 Steeves and Bailey
- 17 Steeves and Bailey
- 18 Slane and Laglois
- 19 Gratton and Polonetsky
- 20 Gratton and Polonetsky
- 21 BC FIPA

s.21(1)(a)

## ANNEX A: ONLINE REPUTATION: SUMMARY OF SUBMISSIONS

THEME	AUTHOR	STAKEHOLDER COMMENTS	POLICY/RESEARCH COMMENTS
<b>1. Potential Gaps</b>			
Site architecture and consent	Steeves/Bailey	“networked media create a “perfect storm” in which architectures incent disclosure of information by young people that is in turn used in commercial advertising and other marketing material premised on narrow stereotypes. Young people reproduce these stereotypes in order to attract “likes”, but their success or their failure opens them up to conflict with others who monitor and judge their self-representations. Simple consent mechanisms are not enough to protect young people’s privacy in this environment, because networked technologies are now embedded in their social lives, their schools and their paid work. In other words, they have no choice but to accept the terms of use even though they do not agree with them.”	
Consent	Jonathan Obar	For policymakers to recognize and acknowledge that notice and choice policy is a great place to start but an unrealistic place to finish if we are ever to realize digital reputation outcomes that empower and protect digital citizens.	
OPC powers	Avner Levin	To some extent the role of the OPC is and will continue to be limited by the lack of order-making powers. .... The OPC should very much continue to advocate and press for legal changes that would bring about such powers.	
Enforcement	Slane / Langlois	(OPC’s ombuds model is) in keeping with the spirit of granting online businesses that traffic in information and user expression tremendous leeway to self-regulate, and to work out solutions (with OPC guidance) rather than to face regulation and set penalties.” “Safe harbors” were developed to protect true intermediaries and platform hosts from legal liability which they would have no realistic way to monitor (and where such monitoring would be undesirable for users generally). This again was thought to be the best way to preserve the open market for	

s.21(1)(a)

		technological and commercial innovation. More recently, however, the law in Canada and other jurisdictions has been recognizing that online businesses that <i>specifically</i> promote and encourage users to post illegal content should not be afforded the benefit of these otherwise justifiable safe harbors.” Canadian privacy law should be brought in line with international developments.	
Legal recourse out of reach	Avner Levin	“In an era where legal representation and legal remedies are increasingly out of reach of average middle-class Canadians, let alone vulnerable individuals, there is a great need for innovative and affordable solutions that will put some control over their reputation and their personal information back in the hands of Canadians.”	
Legal recourse out of reach	ITAC	In most cases, these existing legal and voluntary mechanisms provide significant protections for Canadians from online defamation and harassment. However, one potential gap in the current approach is the time, effort and expense required to seek legal redress through some of these avenues. We encourage the Government of Canada to establish greater protection for individual reputations online by providing individuals with efficient means of redress through existing legal mechanisms.	
<b>2. Solutions (Policy, Technical, Legal)</b>			
No new solutions required	CMA	<ul style="list-style-type: none"> <li>• PIPEDA already provides a workable framework for management of p.i. – see p 4 for explanation</li> <li>• Many websites and online services have policies and procedures for addressing information that users don’t want displayed or shared ex. ability to delete own posts, remove user comments that violate privacy policies and terms of use</li> <li>• Canadians have rights and protections through other legislation and legal remedies ex. copyright, defamation</li> <li>• A more consistent application of the existing framework would go a long way towards addressing issues identified in the discussion paper.</li> </ul>	
Market Implications	ITAC	If Canada creates a challenging environment for online businesses to	

s.21(1)(a)

		operate, it could result in Canadians not being able to access the same services as users in other jurisdictions. It could also make Canada a less attractive place for entrepreneurs to start a new online business.	
MLATs	ITAC	In some cases, Canada could pursue the creation of Mutual Legal Assistance Treaties (MLATs) to expedite legal processes. However, since the challenges posed by online crime and harassment are not unique to Canada, the Government of Canada should not seek to address them in isolation.	
Education	ITAC	Cyber hygiene education, encompassing everything from protecting your online reputation to cyber security, needs to become a core part of Canada's education system. The OPC, as part of its mandate to educate the public, should launch a public awareness campaign to encourage the public to "think twice" before they post, similar to the 2014 "Stop Hating Online" campaign.	
Reputation management companies	Jonathan Obar	The development and support of representative data management service to act as infomediaries to enable digital citizens the opportunity to delegate responsibility via principal-agent relationship. Representative data managers would be responsible for continuously collecting and patrolling our Big Data while offering individuals a simplified and all-encompassing interface that can be managed and controlled from afar. Services currently operating in the financial sector (Lifelock), and those targeting university students going on the job market (e.g.Rep'n'Up), among others, ought to be the subject of various knowledge translation efforts.	
Reputation management companies	BC FIPA	For those who can afford them, reputation management companies can play a leading role in managing one's information online. As described by Oravec, these are companies that "scout websites that post erroneous or damaging private information, correct or delete that info, or petition Web proprietors to take it down." Many work to "bury" unwanted search results by creating and optimizing neutral or positive results.	
Legal right to Obscurity	BC FIPA	Hartzog and Stutzman raise the idea of using online obscurity as a legal	

s.21(1)(a)

		<p>tool. They suggest that obscurity could either be “conferred as a benefit or provided as a middle ground between total secrecy and complete public disclosure. This is particularly true for information that might be embarrassing but not damaging enough to warrant the full force of robust privacy and confidentiality protections.</p>	
Privacy Controls	BC FIPA	<p>Social networks could give individuals greater control of their online reputations by agreeing to standards for privacy controls that go beyond minimum requirements—so that those controls are stronger, vary less across platforms, and are more easily comparable and understandable to the average user—and agreeing to refrain from making their settings less privacy protective without users’ explicit consent. As well, default settings are powerful, and by starting new users—of social networks, websites, or even browsers—with very privacy-protective settings from which they could opt-out, architects of information-sharing platforms could encourage privacy protection, and give individuals a better sense of the privacy protections they may choose to give up.</p>	
Limiting collection of information	Steeves/Bailey	<p><i>Recognize that being in networked spaces is not optional for young people...</i> even if informed about what corporations were doing with their data young people have no real option but to remain in networked spaces. For that reason, approaches focused solely on requiring further disclosure of corporate practices are unlikely to affect any real change. At a minimum, there should be an easy way to opt out of information collection and platforms should be required to include at least some options for communication that will not be monitored.</p>	
Retention and disposal	Steeves/Bailey	<p>Platform providers should make it easier to get harassing content removed and should not be permitted to keep young people’s data in perpetuity.</p>	
Restrict info flows through educational software	Steeves/Bailey	<p><i>Look beyond social media to the impact of educational software in schools...</i> Policymakers need to prohibit or strictly regulate the flow of the</p>	



s.21(1)(a)

		information captured by educational software especially because it can be used to categorize young people in discriminatory ways.	
OPC compliance role	Steeves/Bailey	<i>Use existing powers to limit corporate collection, aggregation and monitoring of young people's data.</i> The OPC, for example, could use s. 5(3) of PIPEDA <sup>i</sup> to limit such practices on the basis that they are not appropriate in the circumstances. One way of doing this would be to require corporations to offer young people the right to opt out of use of their personal information for behavioural targeting. Taking such an approach would assist in breaking the corporate commercial cycle of using young people's data as the basis for profiles that are then used to embed advertising in their social interactions in networked spaces. “	
Education - All groups	TELUS	<ul style="list-style-type: none"> <li>• “Creating an ongoing dialogue with Canadians of all ages about Internet safety, including online privacy and reputation, through in-person seminars and providing educational materials via various media...is essential.”</li> <li>• Advocates collaboration between government and industry to develop and share educational resources</li> </ul>	
Education - Youth	Media Smarts	<ul style="list-style-type: none"> <li>• “Need to foster empathy in online contexts and to teach youth to think ethically and responsibly about sharing other people's content”</li> <li>• “Canadian youth are more likely to turn to teachers and parents for information than to peers or online resources.”</li> <li>• “Need to provide teachers with professional development in digital issues and to ensure that a comprehensive approach to digital literacy is embedded in the K to 12 curriculum of each province and territory.”</li> <li>• “Parents need to be given accurate information, be reassured that their traditional roles as caregivers and moral guides are not only still relevant but more essential than ever, and given practical tools for starting and maintaining conversations with their children on digital issues.”</li> <li>• “Further research into youth norms and attitudes on privacy needs to be conducted, particularly on those areas where it overlaps with other aspects of digital literacy.”</li> <li>• “Parents, healthcare providers, public health authorities, youth advocates and counsellors, community groups and even media</li> </ul>	<ul style="list-style-type: none"> <li>•</li> <li>•</li> <li>•</li> </ul>

s.21(1)(a)

		producers need to be supported in ensuring youth receive a comprehensive education in digital literacy.”	
Education - Youth	FOSI	“Ideally, resilient and informed children would make wise personal choices about the information they share about themselves, the content they post about others, and the way in which they interact publically on the Internet. It is vital to teach children both media and digital literacy, with attention to the importance of their online reputation, both now and in the future.” ... “They should be taught to use the tools and settings already available to help them manage their own content and reputation.”	<ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul>
Education - Teachers	FOSI	“Superior technology training must be provided to all teachers. This will enable them to incorporate digital citizenship teaching across the curriculum, helping children navigate the online world safely and to create positive online reputations at school which will, in turn, provide them with the skills to operate in an increasingly technical world.”	<ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul>
Legislative Solutions – amend PIPEDA (AMPs and order making powers)	Slane and Langlois	<ul style="list-style-type: none"> <li>• Businesses that specifically encourage and profit from users posting sensitive personal information of others where that information damages online reputation, should be made liable under PIPEDA. Liability could be determined using the copyright model framework.</li> <li>• The OPC be empowered to a) issue orders that enjoin businesses that violate PIPEDA from carrying on with those practices, and b) impose administrative monetary penalties (AMPs).</li> <li>• The OPC should be granted greater enforcement power, along the lines of those granted to the FTC.</li> </ul>	[REDACTED]
Work with provinces	Slane and Langlois	There may be avenues for strengthening coordination between provincial consumer protection enforcement and the OPC	[REDACTED]
<b>3. Right to be forgotten</b>			[REDACTED]
Application of PIPEDA	CMA & Bricker et al	No legislative basis for RTBF in PIPEDA	
Application of PIPEDA	Bricker <i>et al</i>	PIPEDA not procedurally adequate for the task of administering hundreds of thousands of complaints that will be submitted to OPC	

Scope of RTBF	BC FIPA	best to aim to only legislate against unwanted behaviour, not things that can lead to it or that allow for it. It is extremely important to avoid overreaching and potentially criminalizing legitimate free expression, or creating a chilling effect on Internet users.	
Application of PIPEDA	David Fraser	“it is wrong in principle to allow information to remain on the internet but to only prohibit a completely uninvolved party from indexing and including it in search results. It is clear that a crucial aspect of the debate over online reputation online is the debate who controls, in what manner, and in what circumstances, the personal information that forms this reputation. Such a framing should, in turn, assure the OPC that a clear mandate for intervention on the basis of PIPEDA does exist not only against information controllers that seek to profit from the reputation they create, such as Globe24h, but more importantly against intermediaries that are commercial in nature, present in Canada, and play a much more significant and amplifying role in terms of bringing reputational-relevant information to the attention of individuals.	
Application of PIPEDA	Chris Berzins	<ul style="list-style-type: none"> <li>• “... there is a reasonable argument that in providing responses to name based search inquiries, search engines such as Google are involved in the collection, use, and disclosure of personal information which is clearly done without the consent of the individuals in question.”</li> <li>• No exemptions apply : info collected by Google is not publicly available under PIPEDA and there is no journalistic purpose</li> </ul>	
Application of PIPEDA	David Fraser	<p>Indexing retrieval and serving of search results are not part of a commercial transaction To begin with, search engines are likely not engaged in commercial activities, at least for the purposes of section 4(1)(a) of PIPEDA because search engines</p> <ul style="list-style-type: none"> <li>• don't charge individuals to search</li> <li>• don't charge content providers to be indexed</li> </ul> <p>In order for PIPEDA to apply to any activity, the collection, use and disclosure of personal information must be in the course of</p>	

		<p>“commercial activities.” One cannot simply say that a search engine is a private commercial undertaking because the definition is not as broad as it seems. As found by the Federal Court in <i>State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada</i>, 2010 FC 736</p>	
Application of PIPEDA	David Fraser	<p>“The indexing, retrieval and serving of search results are not part of any commercial transaction. Ultimately, the search engine is about facilitating timely and easy access to information on the world wide web, which is not an inherently commercial activity. It can most readily be likened to compiling a card-catalogue for a library, but it is electronic and the library is the global internet.”</p>	
Application of PIPEDA	David Fraser	<p>“Search engines are fundamentally journalistic or literary operations, particularly when providing a user with access to news media content. At the same time, they are also providing news media producers with access to readers. The <i>Torstar</i> case was abundantly clear that writing on matters of public interest is not reserved to the mass media. <i>Grant v. Torstar Corp.</i>, 2009 SCC 61 (“<i>Torstar</i>”)</p>	
Charter – Freedom of expression & commercial expression	CMA	<ul style="list-style-type: none"> <li>• “A RTBF would generally deprive listeners and commercial organizations in the interest of protecting individuals.”</li> <li>• Website publishers would be constrained in reaching audiences</li> </ul>	
Charter – Freedom of expression	David Fraser	<p>“Here we are not only concerned with a search engine operator’s constitutionally protected right to freedom of expression, but the right of every Canadian to get access to relevant content on the internet via the use of Google’s search engine. This also limits Canadian media outlets’ constitutionally protected right to disseminate its expressive content on the internet.”</p>	
Charter – Freedom of expression	Gratton / Polonetsky	<p>“Although it is difficult to predict how Canadian courts would rule on this issue, we believe that the approach adopted in Europe would likely be considered unconstitutional. While Canadian constitutional law allows for</p>	

		reasonable limitations of fundamental rights, a European-style RTBF could hardly be justified under the criteria adopted by Canadian courts. In our view, it fails to strike an appropriate balance between freedom of expression and privacy.”	
Charter - Freedom of expression	Gratton / Polonetsky	<p>a RTBF would infringe the constitutional right to freedom of expression of:</p> <ul style="list-style-type: none"> <li>• search providers - “ Search engines retrieve information from an immense pool of data, organizing and ranking such information by displaying results. In our view, there is little doubt that the Charter protects these results as matters of “expression”. Indeed, the Supreme Court of Canada has already stated that hyperlinks “communicate that something exists”. Such an activity undeniably conveys “meaning” that falls within the scope of section 2(b).</li> <li>• authors - authors’ constitutional right to freedom of expression would likely be violated if a statutory RTBF was to prevent search engines from displaying results pointing toward their works. Indexation on search engines has become invaluable for anyone wishing to disseminate information</li> <li>• webmasters - “Webmasters play a key role in disseminating the works of the authors and they equally have an interest in having the public access their webpages freely</li> </ul>	
Charter – freedom of expression	Google	The impact on free expression should be considered, e.x. breaking links to news articles.	
Charter – Freedom of expression	Globe and Mail	RTBF would erode freedom of expression. The appropriate balance between freedom of expression and privacy is already provided for under PIPEDA, defamation law and privacy torts.	
Charter – Freedom of expression	Reporters Committee for Freedom of the Press	<ul style="list-style-type: none"> <li>• International free expression would not survive on the Internet if every nation’s laws apply to every website</li> <li>• RTBF is a European principle that is fundamentally inconsistent with Canadian and international values of free expression</li> </ul>	
Charter – Freedom of expression	Canadian Journalists for Free Expression	RTBF is a threat to press freedom and has no place in Canada.	
Charter – Freedom of	Globe and Mail	<ul style="list-style-type: none"> <li>• The responsibility for appropriately balancing interests should not be</li> </ul>	

expression		<p>transferred from the Courts to multinational corporations.</p> <ul style="list-style-type: none"> <li>• RTBF would erode freedom of expression.</li> <li>• The appropriate balance between freedom of expression and privacy is already provided for under PIPEDA, defamation law and privacy torts.</li> </ul>	
Charter – right to access information & public policy implications	CMA	<ul style="list-style-type: none"> <li>• Internet searches would be incomplete and less relevant information would be surfaced, with significant implications for individuals, organizations and public policy decision making.</li> <li>• RTBF is contrary to public policy objectives as history is rewritten or obliterated, scope of potentially relevant information is limited.</li> </ul>	
Charter – freedom of expression Public Right to Access	David Fraser	Here we are not only concerned with a search engine operator's constitutionally protected right to freedom of expression, but the right of every Canadian to get access to relevant content on the internet via the use of Google's search engine. This also limits Canadian media outlets' constitutionally protected right to disseminate its expressive content on the internet.	
Charter – freedom of expression, Public Right to Access	Canadian Journalists for Free Expression	RTBF is used as a tool by wealthy and powerful individuals; makes it harder for dissidents and journalists to reach the public and leaves citizens less well informed. RTBF is a threat to press freedom and has no place in Canada.	
Charter – separation of powers	David Fraser	<p>Cites <i>General Motors of Canada Ltd. V. City National Leasing, (1989) 1 SCR 641, 1989 CanLii 133</i> and five factors of the valid exercise of the general Trade and Commerce power, specifically that legislation must be concerned with trade as a whole rather than a particular industry or commodity. Argues that :</p> <p>“PIPEDA itself rests on a tenuous foundation, as it does not regulate the economy or trade as a whole, but one singular commodity: personal information. Nevertheless, the application of a “right to be forgotten” would rest on an even more shaky foundation as it would be regulating one activity: the operation of internet search engines.”</p>	

Charter – Public's right to correct information	David Fraser	I also note that such a finding would legally compel a search engine operator to provide incorrect information to its users, which is a disproportionate effect on freedom of expression. ...Omitting a highly relevant, responsive search result would mislead that user into believing that certain content does not exist, though it continues to exist and remains accessible on the media outlet's site. This is akin to a student asking a research librarian for everything the library has about a specific individual, but legally requiring the librarian to lie to the patron. The book would remain on the shelf, but the librarian is prohibited from mentioning it.	
Content Provider Rights	David Fraser	Any process needs to also appreciate that the content provider's interests are also at stake. Content providers choose to make their materials available online and also choose whether to allow it to be indexed by search engines. Meddling with how such content appears in search engine listings interferes with the ability of content providers to reach their intended audiences.... Doing so without their input is very problematic: At the very least, content providers will need to be consulted to provide input on whether the content is "newsworthy". However, placing the search engines as the arbiters of the content provider's rights is not fair to the content provider.	
Reinstating Relevant Information	David Fraser	"how can one revive forgotten information that becomes relevant again"	
Search engine should not be the decision maker	David Fraser	Too great a burden on search engines	
Search engine bias Barrier to market entry	Google	<ul style="list-style-type: none"> <li>• Difficult value judgements with incentive skewed toward removal</li> <li>• Barrier to entry for new search engines</li> </ul>	•
Roles: Search engine should not be the decision maker - Cost	BC FIPA	"Further, there are significant financial costs for carrying out this responsibility. The costs of implementing systems for members of the public to request that their information be obscured or removed, of employing professionals to make these decisions, and of insuring themselves against any fines for potential mistakes will have to come from somewhere. These additional costs could prevent smaller	

		companies and new market entrants from being able to operate or compete effectively, or could translate to additional costs for consumers”	
Roles: Search engine should not be the decision maker – Cost/Time	ITAC	ITAC does not support the introduction of an EU style “right to be forgotten” that would require search engines to evaluate individual requests for specific search results to be blocked based on Canadian privacy law... Requiring search engines to accommodate requests in the subjective space of online reputation is much more complex and costly for search providers”	
Search engine bias Notification of take down requests	BC FIPA	“intermediaries have a documented tendency to “avoid risk and transaction costs by simply removing any challenged content.” As Daphne Keller explains, “Putting removal decisions in the hands of technology companies – as opposed to, say, content creators or national courts – is a recipe for over-removal of lawful expression.  Content creators and hosts should be notified of takedown requests and have the opportunity to dispute them.	
Over-blocking from RTBF-copyright example	Gratton / Polonetsky	“Fair use advocates believe that companies prefer to avoid liability and quickly take down legal content, and thus tread on the rights of those posting content. Wordpress.com has stated that “[t]his isn’t just an outlier case; given our unique vantage point, we see an alarming number of businesses attempt to use the DMCA takedown process to wipe criticism of their company off the Internet.”	
Search engine bias	CMA	Chilling effect on public availability of information as search engines will remove information to minimize liability.	
Roles and Responsibilities	BC FIPA	“If a Canadian right to be forgotten is to be considered to advance this personal data protection, we recommend that the OPC and other policy and law makers exercise great caution in assigning responsibility for it.”  “that the interests of private companies do not necessarily align with the public interest, ... (2) that putting the onus on search companies and other intermediaries could be harmful to the digital economy, and ... (3) that	




s.21(1)(a)

		<p>companies are often risk-averse, and may err towards censorship to protect themselves.”</p> <p>“FIPA recommends that any measures taken to address online reputation concerns be handled by an appropriately-resourced body that is accountable to the public. The actions and decisions of this body should be the subject of robust oversight, including audits designed to ensure obscenity measures and takedowns are used appropriately.”</p>	
Other issues with RTBF	BC FIPA	<ul style="list-style-type: none"> <li>• Inequality will be created between those who know how to look for information and those who do not</li> <li>• How to protect against erroneous or malicious takedown requests</li> <li>• How to enforce outside Canada</li> </ul>	
Practical solution: Standardize Take-Down Request Process and notify source	BC FIPA	<p>“Another consideration is that allowing different websites to set up different processes for requesting or disputing a takedown may create confusion for users, and deter less technologically-literate people from using the system at all.”</p> <p>When someone wishes to have information about them removed or obscured, the process should be relatively simple and standardized across platforms, and the evaluation criteria should be clear. Whenever possible, the content creators or hosts should be notified and given the opportunity to dispute any removal or obscenity requests based on their own rights and interests or a public interest, and sufficient time should be taken to consider the legitimacy of the requests.</p>	
Recommendation- Education re Notification to Internet Users that Information has been omitted	BC FIPA	<p>If it is decided that lawful content can be removed or obscured to protect reputational interests, public education efforts should be made so that Internet users know that information may be omitted from their searches or browsing. As privacy lawyer David Fraser has noted, “A search is ‘tell me what is out there about X’ and an omission without notice is a lie.”</p>	
Proposed solution – better takedown procedures	Gratton/Polonetsky	<p>Develop simpler, cheaper, faster process for online content removal.</p>	

s.21(1)(a)

<p>Proposed solution – availability of PI in public records Alternative – Takedown procedures</p>	<p>Gratton/ Polonetsky</p>	<p>we believe these measures to be very efficient, since their application would force a case-by- case analysis of the limits to freedom of expression, and, because successful application of the measures would see the impugned information totally removed from the Internet instead of its reference in a search engine simply being removed. In addition ..., the individual concerned can still claim damages, in cases in which the comments infringed his or her privacy or reputation.</p>	
<p>Concerns over freedom of speech, role of companies, practicality. Proposed solution – better takedown procedures</p>	<p>FOSI</p>	<p>“FOSI appreciates the intent of lawmakers who consider these approaches to keep children safe online, however we are not supportive of the idea. The approach raises significant questions about freedom of speech and expression, and the role of companies in deciding what information to remove. The global nature of the Internet makes any attempts to limit content accessed in a particular territory extremely difficult, and thus the effectiveness of these rules is brought into question.”</p>	
<p>Recommendation: Transparency Reporting</p>	<p>BC FIPA</p>	<p>“Further data should be collected about online reputation’s effects on the online and offline lives of individuals. Any new policy or law that introduces takedown or obscurity requests should be accompanied by transparency reports with statistics on the number and nature of those requests, and should be subject to regular review.”</p>	
<ul style="list-style-type: none"> <li>• scope</li> <li>• Impact on transparency reporting by public bodies.</li> <li>• PIPEDA - jurisdiction.</li> </ul>	<p>Christopher Berzins</p>	<ul style="list-style-type: none"> <li>• “in my view, Canadian privacy legislation does provide a number of avenues to advance such claims. That being said, without some statutory direction, the challenges in implementing a right to be forgotten are considerable.”</li> <li>• “unlike La Vanguardia, some “publishers”, such as public bodies, will not be able to defend a complaint based on journalistic considerations. Therefore, one should not unduly circumscribe the potential impact of <i>Google Spain</i>; the logic may extend to public bodies posting information on the Internet for a variety of transparency and regulatory related purposes”</li> <li>• “... there is a reasonable argument that in providing responses to name based search inquiries, search engines such as Google are involved in the collection, use, and disclosure of personal information</li> </ul>	

s.21(1)(a)

<ul style="list-style-type: none"> <li>• PIPEDA - exemptions</li> </ul>		<p>which is clearly done without the consent of the individuals in question.”</p> <ul style="list-style-type: none"> <li>• “it is questionable whether any of the exclusions or permissible disclosure provisions in Canadian privacy legislation would apply to a search engine’s activities. For example, it would seem to be a stretch to fit this activity within the exclusion for artistic, journalistic, or literary purposes. It is equally questionable whether this activity would fit within the <i>PIPEDA</i> provisions that allow an organization to collect publicly available personal information without consent, given that the provision of name based search results arguably would not “relate directly” to the purposes for which the information was made publicly available.”</li> </ul>	
<p>Public bodies</p>	<p>Chris Berzins</p>	<p>Considerations in evaluating removal requests to public bodies:</p> <ul style="list-style-type: none"> <li>• Legislative authority and consistent purpose</li> <li>• Administrative tribunals</li> </ul>	
<p>Charter – Freedom of expression</p>	<p>Gratton / Polonetsky</p>	<p>“Although it is difficult to predict how Canadian courts would rule on this issue, we believe that the approach adopted in Europe would likely be considered unconstitutional. While Canadian constitutional law allows for reasonable limitations of fundamental rights, a European-style RTBF could hardly be justified under the criteria adopted by Canadian courts. In our view, it fails to strike an appropriate balance between freedom of expression and privacy.”</p>	
<p>Charter – Scope of the CHRF</p>	<p>Gratton / Polonetsky</p>	<p>“Section 2(b) of the Canadian Charter provides that everyone has the fundamental freedom of expression, including freedom of the press and other media of communication. The Charter is subject to a “purposive” and “generous” interpretation, which is meant to give full effect to the civil liberties that it guarantees. Freedom of expression is no exception. The notion of “expression” has been construed very broadly, so as to include any activity that attempts to convey meaning, including both form and content.”</p>	
<p>Future Challenges with Implementation of RTBF</p>	<p>Gratton / Polonetsky</p>	<p>“First, the constant evolution of social norms would lead to the erasure of certain information that was unacceptable at the time of the erasure, but</p>	

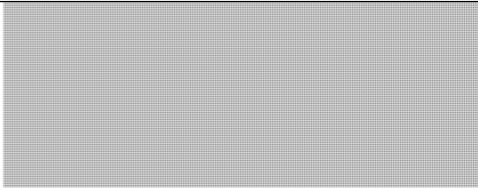

		that, over time, may gradually become acceptable or at least, less relevant ... Second, the unequal implementation of a RTBF across different jurisdictions could ultimately lead to an extraterritorial application of the RTBF.”	
Oakes Test –pressing and substantial objective	Gratton / Polonetsky	<p>“Authors, webmasters and members of the public are not notified of a complaint and have no way to intervene and demonstrate that the information is adequate and relevant. In fact, search engines have no obligation to alert page owners of the delisting. Moreover, while claimants can resort to privacy authorities and to the courts if dissatisfied with the decision, nobody else can challenge it. This one sided approach is a blatant breach of the most basic principles of procedural fairness, and Canadian courts would most likely consider this aspect if and when called upon to determine whether or not the RTBF could be justified under section 1 of the Charter.”</p> <p>Would also fail on proportionality because a “RTBF would cover information far remote from the value of privacy which underlies the Canadian Charter.” For example, “a RTBF would extend to personal information which is not intrinsically private, including information pertaining to the claimant’s public activities.” “Conversely, search engine results contribute to the core purposes of the constitutional right to freedom of expression, namely democratic discourse, truth-seeking and self-fulfillment.”</p> <p>“The first step requires assessing whether the objective of the infringing measure is sufficiently important to justify overriding freedom of expression... The objective of a RTBF could be described as providing an individual with some measure of control over personal information that is disseminated on the Internet and that creates a risk of harm.<sup>91</sup> Such an objective is connected to fundamental values, such as privacy, dignity and autonomy. In all likelihood, this objective would be recognized as sufficiently important to justify a limit on freedom of expression.”</p>	
Oakes Test – Rational connection between the law	Gratton / Polonetsky	“With respect to the RTBF, the ability to request the delisting of certain links from search results is undeniably connected to the objective of	

and its objective		empowering individuals, so that they can better control the dissemination of their personal information on the web. The rational connection requirement would therefore not, in our view, be the subject of extensive debate.”	
Oakes Test– Proportionality & proposed solution	Gratton / Polonetsky	“In our view, the benefits of delisting “personal information” that is not inherently private and that causes no harm cannot outweigh the deleterious effects on freedom of expression, especially considering that authors and webmasters will have no say as to the relevance and adequacy of the information in question. We therefore believe that a RTBF would fail to satisfy the last stage of the Oakes test, even assuming that the minimal impairment test is met. However, a limited RTBF might possibly strike an appropriate balance between freedom of expression and privacy if limited to intrinsically intimate information which creates a significant risk of harm. Moreover, such a policy might be much more justifiable if, instead of leaving its enforcement to search engines, legal mechanisms were set up to allow authors, publishers and members of the public to assert their rights. “If the RTBF was tailored so as to apply exclusively to intrinsically intimate and significantly harmful information (the victims of revenge porn come to mind), its benefits might justify such purposive limits on the freedom of expression.”	
Procedural fairness	Gratton / Polonetsky	“Search engines are biased in favour of the claimant, thus increasing the likelihood that information of public interest being removed from search results. Authors, webmasters and members of the public are not notified of a complaint and have no way to intervene and demonstrate that the information is adequate and relevant. In fact, search engines have no obligation to alert page owners of the delisting. Moreover, while claimants can resort to privacy authorities and to the courts if dissatisfied with the decision, nobody else can challenge it. This one-sided approach is a blatant breach of the most basic principles of procedural fairness, and Canadian courts would most likely consider this aspect if and when called upon to determine whether or not the RTBF could be justified under section 1 of the Charter”	
RTBF – Role of individual	Gratton / Polonetsky	“In our view, the claimant should have the burden of showing that the	

		dissemination of his/her personal information definitely causes a certain harm or, at the very least, a risk of harm; otherwise the public interest to be informed should prevail over any such purely private interest.” Under certain circumstances, such a requirement might help prevent the removal of information relevant to the public.”	
RTBF - Alternative Solutions	Gratton / Polonetsky	“a limited RTBF might possibly strike an appropriate balance between freedom of expression and privacy, if it was limited to intrinsically intimate information which creates a significant risk of harm. Moreover, such a policy might be much more justifiable if, instead of leaving its enforcement to search engines, legal mechanisms were set up to allow authors, publishers and members of the public to assert their rights.”	
Alternative Solutions: PIPEDA - evolution of the existing legal framework	Gratton / Polonetsky	<p>“Data protection laws, such as PIPEDA and substantially similar provincial laws, already include, to a certain extent, the principle underpinning the right to be forgotten. Like Directive 95/46/EC, these laws already cater to a RTBF in Canada, through certain rights and principles such as the data collection limitation principle (prohibiting an organization from collecting more personal information than <i>necessary</i> for the purpose identified) as well as the data use, disclosure and retention limitation principle (precluding an organization from using or disclosing more personal information than <i>necessary</i> for the purpose identified)“</p> <p>Also cite evolution of cyberbullying and revenge porn laws as obviating the need for a RTBF.</p> <p>Notwithstanding the constitutional challenges already discussed above, while Canadian data protection laws could, to a certain extent, play the role of legitimizing a RTBF in Canada, in the same way as Directive 95/46/EC and the related Data Regulation have in Europe, some authors have argued that the expansive definition of “personal information” dilutes its effect and undermines its main objective.”</p>	
Legislative solutions – Quebec defamation law	Gratton / Polonetsky	individuals’ reputations are better protected with the Quebec legal framework, given that the personal information that is revealed to the public must not only be true or accurate; it must also be necessary to convey the particular content in which the public has a “legitimate	

		interest”. This type of additional layer of protection is helpful to further enhance the protection of individual reputations and should be studied by legislators in other provinces before they consider implementing a RTBF.	
Legislative alternatives – clean slate laws & employment law	Gratton/Polonetsky	Enhance laws that restrict the availability and use of personal information. Ex. clean slate laws like bankruptcy law, juvenile criminal law and credit reporting allow for deletion of negative information about a set period of time; employment laws prohibit asking for social media passwords by prospective employers“	
Individuals’ access to information	Gratton / Polonetsky	“Information is the main asset of the current digital era where we live and a powerful tool; that is why the access to information should be a fundamental right for all citizens, and not only for some of them. Making it difficult for certain citizens to access certain information, has the risk to place them in a disadvantaged situation. A RTBF in Canada would lead to unequal access to data.”	
Concerns over freedom of speech, role of companies, practicality.	FOSI	“FOSI appreciates the intent of lawmakers who consider these approaches to keep children safe online, however we are not supportive of the idea. The approach raises significant questions about freedom of speech and expression, and the role of companies in deciding what information to remove. The global nature of the Internet makes any attempts to limit content accessed in a particular territory extremely difficult, and thus the effectiveness of these rules is brought into question.”	
Suggestion for implementing the RTBF	Google	Any framework must have transparency, accountability and recourse mechanisms.	
Recommendations for how to implement	ITAC	<ul style="list-style-type: none"> <li>• Develop a national consensus on who and what is eligible to be “forgotten”</li> <li>• Any “right to be forgotten” should be overseen and impartially administered by a government appointed regulator based on clear principles articulated through legislation passed by Parliament</li> <li>• Restrict any domain or search restriction rulings to Canadian (.ca)</li> </ul>	

s.21(1)(a)

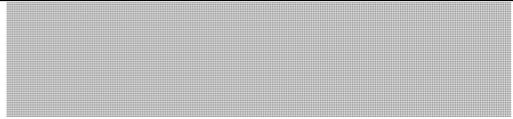

		variations	
Recommendations for how to implement	Bricker <i>et al</i>	RTBF will need to be implemented through legislation, will need to target specific types of problematic online activity, and provide affected individuals with recourse through the courts.	
OPC should investigate	Avner Levin	"...the OPC should not shy away from investigating, finding and if necessary asking the court for an order that the Right to be Forgotten exists in Canada as well. The litigation against Globe24h will hopefully help set a precedent in this regard."	
In favour of idea of RTBF	Dr. Jenn Barrigar	"This ruling isn't the creation of a new form of censorship or suppression – rather, it's a return to what used to be. It aligns new communications media with a more traditional lifespan of information and restores eventual drawing of curtain of obscurity as timeliness fades."	
Charter – public's right to information	Canadian Journalists for Free Expression	RTBF is used as a tool by wealthy and powerful individuals; makes it harder for dissidents and journalists to reach the public and leaves citizens less well informed.	
<b>4. Vulnerable groups</b>			
Disadvantaged groups	Johnathan Obar	Suggests the development of policies ensuring representative data management services are targeted towards communities more likely to be the subject of Big Data-driven discrimination.	
Women, girls, visible minorities	Media Smarts	<ul style="list-style-type: none"> <li>• "Many online spaces are hostile environments for women and girls, as well as for visible minorities and other marginalized groups...youth need to be made aware of their rights in online spaces and empowered to build communities where their rights are respected."</li> <li>• (With regard to gender) "Ethics training...must be supplemented with a rights-based approach to digital citizenship, in which students are taught the importance and inalienability of the right to privacy and to give and withhold consent ... and are encouraged to question attitudes towards gender and sexuality..."</li> </ul>	<ul style="list-style-type: none"> <li>• </li> <li>• </li> </ul>



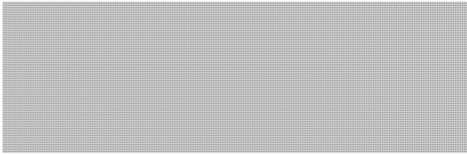

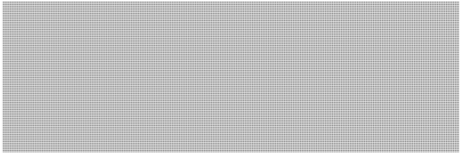

s.21(1)(a)

<p>First Nations, LBGTQ, high risk youth, seniors</p>	<p>TELUS</p>	<p>It is strongly recommended that the OPC make a special effort to reach out to organizations that work with vulnerable individuals and marginalized communities—and when appropriate, to those individuals and communities themselves—in order to get a fuller picture of how and why they participate online, what their specific needs are, and how they feel they should be protected Education should be customized for First Nations, LBGTQ, high risk youth (e.g. kids leaving foster care) and seniors.</p>	<ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul>
<p>Disadvantaged groups</p>	<p>BC FIPA</p>	<p>Human rights law and employment standards laws should be considered as possible vehicles for protecting disadvantaged groups and individuals who suffer as a result of damage to their online reputation. Perhaps improvement to these laws should be considered before seeking to introduce altogether new legislation.</p>	<ul style="list-style-type: none"> <li>• [REDACTED]</li> </ul>
<p>Young women, LBGTQ</p>	<p>Steeves / Bailey</p>	<p>“The eGirls Project participants understood girls and young women and members of the LBGTQ community to be particularly vulnerable to disabling attacks on their reputations.<sup>ii</sup> As a result, some felt it would be particularly important to address discrimination and prejudice through educational measures to combat homophobia, misogyny and other forms of oppression. Policymakers need to think more carefully about privacy for members of equality-seeking communities.”</p>	
<p>Women</p>	<p>Slane/Langlois</p>	<p>“(revenge porn) sites radically transform the online reputation of the subject of shaming, so that it is difficult for her (as most are women) to craft a reputation that is not primarily defined by non-consensually shared pictures of a private nature. As such, informational violence has been done to the subject’s online and offline subjectivity, defined as it increasingly is by the matrix of data points and their interpretation in myriad contexts.”</p>	
<p><b>5. Responsibility/Roles of Players</b></p>			
<p>Role of individual v role of</p>	<p>Dr. jenn barrigar</p>	<ul style="list-style-type: none"> <li>• Argues that PIPEDA stems from the wish to protect economic and</li> </ul>	

s.21(1)(a)

organization		<p>commercial interests rather than the desire to protect privacy.</p> <ul style="list-style-type: none"> <li>• Critiques what she perceives as the offloading of responsibility from government to the individual (“responsibilization”)</li> <li>• “...there is a clear movement towards a focus on individual agency and responsibility, with its attendant demonization and disdain for the “stupid user” individual who fails to exercise the requisite agency and protect themselves.”</li> </ul> <p>“...with so many sites online dependent on personal information and reputation to facilitate user interaction and revenue generation, an odd balance is struck where the information models of these spaces remain unquestioned and the actions of those who use them are problematized instead.”</p>	
Policymaker role	Steeves/Bailey	Rather than focusing on individual roles and responsibilities, policy makers should pay more attention to corporate practices and policies that compromise individuals’ ability to negotiate privacy in networked spaces.	
OPC Role	Avner Levin	At the same time the OPC should advocate for the creation of more hybrid regulatory-driven/technologically-enabled solutions such as online removal-request forms that should highly appeal to Canadians – and to the private sector – because of their low costs and ease of use. Creating online, even partially automated or algorithmic-run processes would improve the management of reputation for a great number of individuals and would alleviate the need for ad-hoc interventions on behalf of the regulator.	<ul style="list-style-type: none"> <li>• </li> </ul>
Social sharing platforms	Tim Banks <i>et al</i>	The submission examined the tools provided by 38 social sharing platforms such as social media, dating and alternative news sites to manage reputation. The focus was to consider how these sites used community standards and takedown policies to balance rights of freedom of expression with other values, and how takedown tools may affect the ability of an individual to protect his or her reputation. The authors concluded that social sharing platforms have a role in helping balance online reputational rights and other values. However, at present, the tools provided to users are not sufficient.	<ul style="list-style-type: none"> <li>• </li> </ul>

s.21(1)(a)

<p>Platforms – liability and takedown mechanisms</p>	<p>Tim Banks <i>et al</i></p>	<p>“... although the user may be acting for non-commercial purposes, the platform, as a professional service provider, may be engaged in commercial activities while processing and distributing information on behalf of a the user. Can such a platform distance itself from improper use of personal information by a user if the platform provides no mechanism to address improper use?”</p>	
<p>Roles of individuals, gov’t , industry</p>	<p>TELUS</p>	<p>“... individuals must play a key role in taking responsibility for our online privacy and reputation...it is critically important that we, as individual Canadians, understand the online products and services we use and the implications of sharing or “publicizing” information about us and others...it is the responsibility of a wide variety of groups and institutions (industry, government, law enforcement, education and topic experts) to collaborate on educating Canadians on this important topic.”</p>	<ul style="list-style-type: none"> <li>• </li> <li>• </li> </ul>
<p>Roles of companies, parents, the OPC</p>	<p>FOSI</p>	<ul style="list-style-type: none"> <li>• “Cross-sector bodies, ... such as UKCCIS,<sup>16</sup> bring together industry, non-profits, civil servants and ministers from government departments, educators, health professionals and researchers to develop strategies to counteract online challenges and emerging issues. Uniting relevant government departments also allows for consolidated governmental policies and approaches</li> <li>• “The OPC can raise awareness about online privacy and reputation resources so that Parliamentarians can help spread the word and educate their constituencies. The government can also work with other parties to develop and distribute additional resources to help inform consumers.”...</li> <li>• “The OPC should conduct research to examine how people think about online privacy with particular attention to teenagers and online reputation. Research should serve as a foundation for creating policies and developing education in order to reach all populations. Furthermore, the OPC should also ensure that resources and materials are available in multiple languages for a variety of comprehension levels and develop an effective distribution strategy to reach families across Canada.” ..</li> </ul>	<ul style="list-style-type: none"> <li>• </li> <li>• </li> </ul>

- “recommends that the OPC works with all stakeholders to find solutions to help Internet users manage their digital reputation. Government, industry, schools, parents, and organizations should educate users to think before they post and consider the impact of online content on their reputation on and off-line.”
- “As part of this, FOSI encourages robust and comprehensive industry self-regulation and cooperation, incorporating topics such as privacy, reputation, and responses to take-down requests from users.”
- “..Many have formed safety advisory boards, which bring in outside experts to advise companies on a multitude of safety issues, including privacy settings. Some of the best practices to help people deal with their online reputation and privacy include the creation of safety centers, privacy checkups and options for customizing who can view profiles and online content. It is especially helpful when companies provide periodic reminders to consumers to review their settings.”...  
“Technology companies should look to existing industry best practices to create robust technical settings to increase user control. Online platforms should provide educational messaging to help users determine how much and with whom they want to share their information. Companies already offering these features should remind people of the existence their tools and promote their usage to help lessen the risk of online reputational harms.”
- “Engaged and knowledgeable parents are vital to ensuring that children have a safe online experience. Providing and encouraging the use of online safety and privacy tools is a community-wide effort and each player in the online safety ecosystem can play a role in helping parents and kids to learn about and embrace the tools available to them.”

Consultation questions:

1. We have highlighted some potential gaps in protections between the online and offline worlds. What other gaps exist?

2. What practical, technical, policy or legal solutions should be considered to mitigate online reputational risks?
  3. Can the right to be forgotten find application in the Canadian context and, if so, how?
  4. Should there be special measures for vulnerable groups?
  5. Who are the key players and what are their roles and responsibilities?
-

## ANNEX B: Proposed outline for the reputation position paper

The position paper (estimated at 15 pages) would include:

- 1) An introduction that provides an overview of the discussion paper on reputation and call for papers.
- 2) A summary of the submissions received from external stakeholders. This section will outline the solutions proposed by stakeholders by category: education, site architecture, OPC compliance and enforcement, research, and legal options. It will also discuss the RTBF in terms of comments received and the OPC's view on the application of the RTBF in the Canadian context generally and in PIPEDA specifically.
- 3) A discussion of the preferred solutions, including benefits, risks, and strategic considerations. Also included in this section will be the roles and responsibilities of the players, including the OPC, industry, individuals and legislators.
- 4) The OPC's next steps in advancing and promoting measures to mitigate online reputational harms to individuals will be outlined.

Commissariat  
à la protection de  
la vie privée du  
CanadaOffice of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
Unclassified	4

**NOTE D'INFORMATION****BRIEFING NOTE**

***Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada  
(September 2016)***

**OBJET / PURPOSE:** to provide background for discussion on the above-noted report<sup>1</sup> published September 13, 2016 by the Telecom Transparency Project at the Citizen Lab (University of Toronto) and the Canadian Internet Policy and Public Interest Clinic (CIPPIC)

**APERÇU / OVERVIEW:***About the authors and report*

- The report was written by Christopher Parsons (Citizen Lab Research Associate) and Tamir Israel (CIPPIC Staff lawyer) to chart the capabilities of “IMSI Catchers” as well as document efforts by institutions to obscure their use from public record.
- The report also provides a detailed overview of how IMSI devices technically function, the minimal transparency around their use in the UK and US, and description of the legal authorities needed to operate IMSI Catchers in Canada.
- The authors argue the absence of privacy protections governing use of the devices in Canada stems from the broad legal authorities in the *Criminal Code* powers most likely used to authorize their use; they conclude with a series of recommendations to bring use of the devices into compliance with privacy rights and Charter jurisprudence.

*Overview of the technology*

- The report begins with a helpful “IMSI Catcher 101” section (p. 2) to assist the reader in seeing the basic network concepts that the devices exploit in order to carry out tracking and surveillance.
- In essence, a IMSI Catcher is a radio device that masquerades (or spoofs) any mobile device that comes within range into registering with it, treating the installation as if it were a regular telecommunication tower or base station.
- The IMSI Catcher then collects identity, authentication and locational data direct from the target device (or simply all devices that come within its range); this is referred to as ‘identification mode’. Another invasive functionality (‘camping mode’) can enable full packet capture, essentially converting the device into an interception tool (p. 3).
- While installation of user-enabled encryption tools (like PGP, OTR, etc.) can minimize risk of unauthorized access, other device elements cannot be masked and are therefore inherently vulnerable to collection (p. 4)
- The ‘identification mode’ described is most frequently used by police, border security and other law enforcement agencies to map networks of individuals, profile mobile use around certain locations, pick out unknown signals and/or located specific targets (p. 5).

<sup>1</sup> *Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada* – URL: [https://citizenlab.org/wp-content/uploads/2016/09/20160818-Report-Gone\\_Opaque.pdf](https://citizenlab.org/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf)

This is achieved either by using the geo-location functions of the device itself (GPS) or with triangulation (installation of more than one device) (p. 8).

- This mapping feature does not require any conscious usage of a mobile device; all GSM-enabled phones register automatically with cell-towers within range immediately upon powering on, and continue to “ping” nearby stations detected as a signal check while on.

#### *Device functionality and capabilities*

- Bearing these capabilities in mind, the report notes that in the past several years, IMSI devices have been reported to have been used for:
  - Confirming the presence of a suspect inside a building prior to arrest;
  - Tracing the origin of certain communications;
  - Locating certain devices within a particular area;
  - Scanning urban areas (via low-altitude overflight);
  - Monitoring prisoners;
  - Registering individuals at public protests;
  - Profiling activities at oversight bodies (p. 14).

#### *Lack of transparency and accountability*

- The report notes that multiple, and shifting, rationales have been advanced by authorities to maintain secrecy around the use of the devices; this despite the fact that all devices that use public radio spectrum in the US, Canada and UK require official regulatory registration (p. 22); prosecutors in the US and Canada have even abandoned serious criminal cases before the courts to maintain secrecy (p. 24).
- In Canada, the report notes that only superior court officials appear to have actively challenged the scope and terms of IMSI use; oversight bodies, ministers’ staff or Parliamentary bodies have not actively sought reform (p. 25-26).
- In early 2014, for their part, the RCMP responded to written questions from a member of Parliament stating they only use a “mobile device identifier” (MDI) with judicial authorization in specific investigations (p. 28); another RCMP investigator cited in the paper (cited from court testimony) deployed an IMSI catcher in dozens of cases.
- The authors note the incongruity in maintaining official secrecy about IMSI devices, in light of that fact that public reports for the use of other forms of electronic surveillance have been required by law since the 1970s; covert video surveillance and location tracking have been publicly acknowledged since the 1990s.
- In the researchers’ view, official transparency will not compromise the practical utility of the devices (p. 34); rather institutional sensitivity around IMSI Catcher use appears to be more in response to public concern and controversy about surveillance (p. 38).

#### *On legal standards for usage*

- The report highlights the point that both the US Department of Justice and DHS require a warrant (at the probable cause standard) for the use of IMSI Catchers in investigations; these have been set out in public policy documents. There have also been published examples of specific court limitations imposed through IMSI Catcher authorizations (p. 54-55).



- This is in contrast with the state of “opacity” in Canada, where authorities appear to be relying upon general warrants to authorize IMSI Catcher usage; this despite those provisions (*Criminal Code* 487.01) being put in place to fill gaps where no more specific authorization scheme exists (p. 57-58, 73-74).
- Finally, the report contains a very detailed legal analysis of the minimal constitutional standards (post-Spencer) that should be in place for collection of metadata and usage of IMSI Catchers or similar surveillance techniques (p. 83-103).

*Report recommendations*

1. *That annual statistical reporting, individual notification and registration / certification of use should accompany institutional usage of IMSI Catcher devices in Canada (p. 108-116)*
2. *That warrant conditions similar to wiretapping be put in place for IMSI Catcher authorization, namely use in serious criminal cases, requirement to demonstrate investigative necessity, and reasonable grounds to believe as a standard (p. 116-120)*
3. *Courts should impose specific minimization procedures to limit scope of collection, retention of unnecessary data and restrict secondary use (p. 121-125).*

**DISTRIBUTION:** Commissioner, Patricia Kosseim, LSPRTA, Michael Billinger

**APPROBATION / APPROVAL:**

<b>Rédigé par / Prepared by</b>	<b>Date</b>	<b>Revisions</b>
Chris Prince	Sept, 13, 2016	Sept. 20, 2016
<b>Approuvé par / Approved by</b>		
<b>Date</b>		
Barbara Bucknell <i>Directrice, Politiques et recherche / Director, Policy and Research</i>		



Commissariat  
à la protection de  
la vie privée du  
Canada

Office of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
Protected B	9 + Annex A

---



---

## NOTE D'INFORMATION

---



---

## BRIEFING NOTE

---



---

### OBJET / PURPOSE:

To provide you with background information for your meeting with Canada Revenue Agency (CRA) Commissioner Bob Hamilton and the CRA Senior Management Team. The meeting is on November 16<sup>th</sup> 2016.

### APERÇU / OVERVIEW:

#### 1. Biography of Commissioner Hamilton

Commissioner Hamilton was appointed to his position at the CRA on August 1<sup>st</sup> 2016. Prior to joining the CRA he served as:

- Deputy Minister of Environment Canada;
- Deputy Minister of Natural Resources Canada;
- Senior Associate Secretary of the Treasury Board;
- Senior Assistant Deputy Minister, Tax Policy at Finance Canada;
- Assistant Deputy Minister of Finance Sector Policy at Finance Canada; and
- Lead Canadian on the Canada-United States Regulatory Cooperation Council

#### 2. Overview

In terms of main messaging:

- Our Office has seen an increasing number of initiatives involving personal information – these involve the expanding of existing programs and introduction of new programs. Given the growth in new programs and information sharing involving the CRA, lessons learned (from our investigations and recent audit of CRA) highlight the importance for PIAs and updating a privacy management program.
- While our Office does appreciate efforts to combat issues such as tax evasion or money laundering, we have suggested the CRA submit PIAs as early as possible to our Office, and evaluate how it assess risks, including potential secondary uses that may not be clear to taxpayers.
- We have recently seen an increase of PIAs sent to our Office by the CRA – this coincides with our recommendation that the CRA assess risks based on its internal uses of taxpayer information.
- There has been a positive working relationship between their CPO and our PIA officials. As a part of this relationship, the CRA indicated they were in the process of identifying comprehensive program-level PIAs to address recommendations our Office made.
- One of our Office's recommendations to the CRA following our 2013 audit was for the Agency to implement a Chief Privacy Office to coordinate accountabilities, responsibilities, and activities. In 2016, our Office confirmed that the CRA has fully implemented this recommendation - and that it has fully implemented or substantially implemented all of the recommendations made in our 2013 audit.
- We are also pleased that the CRA has worked collaboratively with our Office to distribute, in its regular mail-outs to businesses, an insert about privacy obligations that will reach roughly 500,000 SMEs.



Commissariat  
à la protection de  
la vie privée du  
Canada

Office of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
Protected B	9 + Annex A

### 3. Privacy Act Reform

The House of Commons Standing Committee on Ethics, Privacy and Access to Information (ETHI) has been reviewing both the *Privacy Act* and the *Access to Information Act* (ATIA). The Committee made a series of recommendations to the Government in June 2016 on ATIA reform and an official response from the government was issued in October.

Our Office appeared before Committee and made a case for comprehensive reform of the *Privacy Act* built upon three main observations:

- Technological change: which has allowed information sharing to increase exponentially, while controls have been overshadowed;
- Legislative evolution: where an explicit necessity requirement for collection to protect against over-collection would align PA with other privacy legislation in Canada and abroad;
- Expectations for transparency: examples include extending the Act's application to all institutions, allowing OPC to report proactively and requiring government transparency on lawful access demands.

The *Privacy Act* still has no express legal obligation on the part of its government institutions to safeguard individuals' personal data. While under section 241(1) of the *Income Tax Act*<sup>1</sup> there are confidentiality requirements on CRA employees and others with access to taxpayer information, our last audit of CRA found that there were areas of improvement, notably for employee access rights to taxpayer information, and ensuring more timely assessment of privacy and security risks. CRA responded positively to recommendations made in our audit and indicated that they would be implementing solutions to address those issues.

The CRA<sup>2</sup> appeared before Committee on October 6<sup>th</sup> 2016, and noted:

- Overall, 6 of the 9 recommendations from our Office's last audit of CRA have been implemented, with the remaining 3 to be done by next year.
  - The CRA noted that it has implemented audit controls for employee monitoring of files, and plans to continue to review and update them. It also noted it has increased its employee education programs, including associated communication materials.

<sup>1</sup> Section 241 of the *Income Tax Act*:

*Except as authorized by this section, no official or other representative of a government entity shall*  
*(a) knowingly provide, or knowingly allow to be provided, to any person any taxpayer information;*  
*(b) knowingly allow any person to have access to any taxpayer information; or*  
*(c) knowingly use any taxpayer information otherwise than in the course of the administration or enforcement of this Act, the Canada Pension Plan, the Unemployment Insurance Act or the Employment Insurance Act or for the purpose for which it was provided under this section.*

<sup>2</sup> Appearing for the CRA were Mr. Maxime Guénette (Assistant Commissioner and Chief Privacy Officer, Public Affairs Branch, Canada Revenue Agency, and Marie-Claude Juneau (Director of the Access to Information and Privacy Directorate at the Agency).



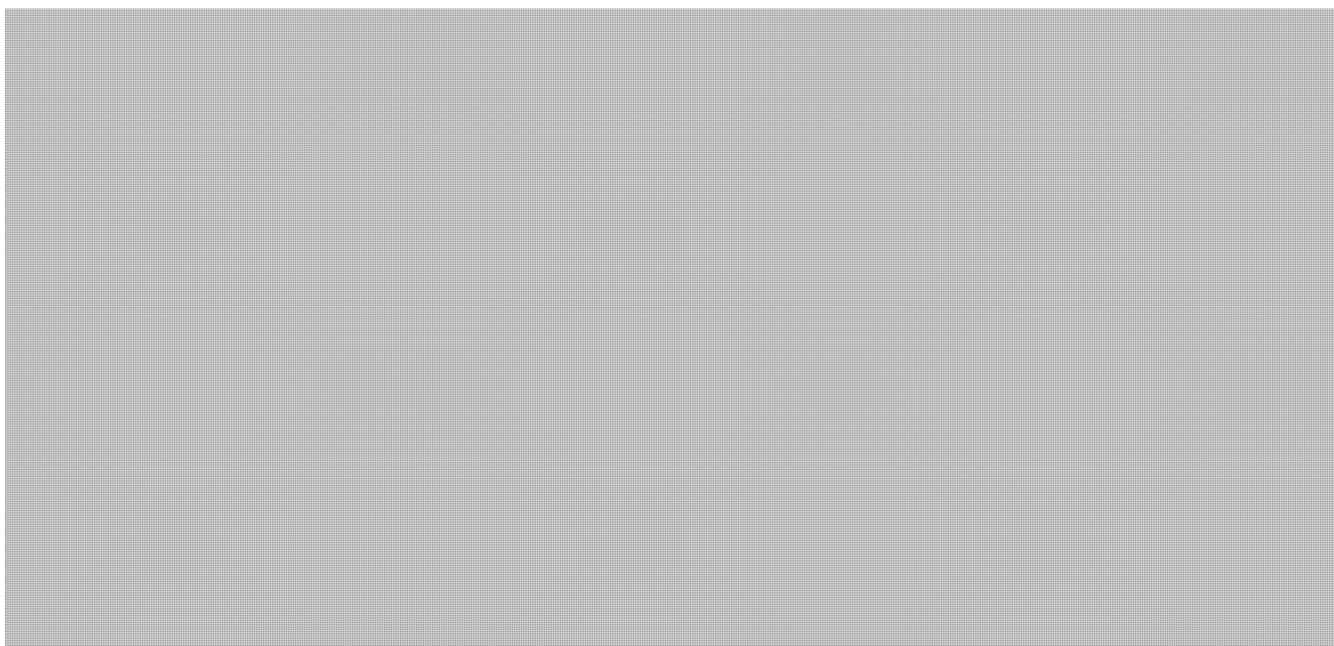
Commissariat  
à la protection de  
la vie privée du  
Canada

Office of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
Protected B	9 + Annex A

- In dealing with the OPC, the CRA indicated that it looks for ways to work with the OPC to resolve issues, and would continue to do so if the legislative framework for the *Privacy Act* was amended.
- The CRA is looking to invest in its information technology services and systems.
- The CRA has completed 16 PIAs this year, and expects to complete 18 more this fiscal year. It also noted it regularly consults with our Office.
- The CRA is aware of the sensitivity of the personal information it holds, and indicated that there “can always be room for improvement”.
- During the question period, the CRA did not provide an opinion on damages, but did note there was no compensation to individuals in the case of a large breach involving taxpayer information.

#### **4. Review of Personal Information handling practices under the *Security of Canada Information Sharing Act (SCISA)***



#### **5. OPC Audit of CRA**

Our audit of the CRA in 2013 found that since our last audit (which was in 2009) the CRA has made progress to strengthen its privacy and security policies and procedures, and to communicate its expectations to employees about the safeguarding of personal information.

The audit report did however note a number of shortcomings:

- PIAs are not always completed before projects are implemented
- The role of the CPO is not formalized
- Generic user IDs that are developed for IT testing are not adequately controlled
- Gaps exist in the monitoring of employee access to taxpayer information
- Threat risk assessments are not completed for many systems

s.16.1(1)(d)

s.21(1)(b)



Commissariat  
à la protection de  
la vie privée du  
Canada

Office of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
Protected B	9 + Annex A

- Access to taxpayer information by IT developers is inadequately monitored
- Serious breaches involving the disclosure of taxpayer information have occurred at the Agency

That said, the report did note that:

- The CRA indicated that it has substantially or fully implemented all measures that we recommended. The Agency reports that it has made several important improvements to its management of personal information, including introducing new policies, increasing corporate oversight and ensuring more timely assessment of privacy and security risks.
- The Agency appointed a Chief Privacy Officer (CPO) in 2013 who is a member of the Agency Management Committee and has a broad mandate for privacy oversight and promotion. The CPO's role includes overseeing decisions related to privacy, including privacy impact assessments; championing personal privacy rights, including the management of privacy breaches; and overseeing privacy awareness, including communications and training activities for all Agency employees.
- The Agency has also enhanced its information technology (IT) controls over taxpayer systems, including improved internal access rights management and monitoring. It also expects in 2017 to fully implement the monitoring controls recommended in our audit.
- Our Office understands the CRA has invested significant funds and is planning a further significant investment to enhance its identity and access management controls.

## **6. Parliamentary Appearances Related to the CRA**

### **Foreign Account Tax Compliance Act (FATCA)**

- FATCA reporting obligations has raised a number of privacy considerations. In addition to briefings from Finance Canada, our Office held meetings with CRA officials to discuss operational/legislative changes, and continue to engage with them on the PIA.
- Our Office appeared three times before Parliament on this issue. The first two instances were in 2014, when the reporting obligations were introduced by Bill C-31 (*Economic Action Plan 2014 Act, No. 1*). More recently, we appeared before ETHI this past April, at the same session as the Minister of National Revenue.
- We continue to have outstanding questions on the regime, and in September 2016 the OPC PIA group sent a letter to the CRA to receive additional information on:
  - details on the safeguards measures to ensure the IRS uses and disposes of personal information provided by the CRA, in accordance with the IGA;
  - the number of records received from the IRS; and
  - If, as a best practice, the CRA will inform impacted individuals of the transfer of their information to the IRS.



Commissariat  
à la protection de  
la vie privée du  
Canada

Office of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
Protected B	9 + Annex A

## Information Sharing between the CRA and Office of the Chief Actuary

- In June 2016, our Office appeared before the Senate National Finance Committee on Bill C-15 (*the Budget Implementation Act 2016, No. 1*). While C-15 contains many amendments to a number of Acts, we were only asked to appear on one clause in the *Income Tax Act* where “taxpayer information” would be shared with the Office of the Chief Actuary of Canada (OCA).
- At the appearance our Office noted that the changes proposed to the *Income Tax Act* by Bill C-15 are meant to facilitate the work of the Chief Actuary and the fulfillment of the associated legislative duties. We, however, raised concerns that the wording could allow for the sharing of taxpayer’s personal information in identifiable form even where anonymized information would suffice. We recommended that privacy protections be outlined in subsequent information sharing agreements.
- Following that appearance our Office met with a number of CRA officials to discuss this issue. As a result of those discussions CRA officials indicated they will provide an update to our Office with respect to the information sharing agreement that would be developed, which will include the data elements that would be shared and privacy protections that would be put in place.
- We were also advised by CRA officials that, given that the information is not for administrative purposes, a PIA may not be undertaken – but if one is it will be shared with our Office.

## 7. Privacy Impact Assessments

Our Office has received 29 new CRA PIAs since April 1, 2014. This represents 11 % of the overall total of 252 PIAs and Consultations we received in the same time period.

That said, we have received 20 new PIAs from CRA this fiscal year alone. Many of these new CRA PIAs are for activities that have been underway for a number of years (for example, the Criminal Investigations Program, Collection and Verification, Business Intelligence and Compliance, Canada Child Benefits, Film & Media Tax Credits Program).

This increase coincides with our recommendations to assess the risks of internal use of taxpayer information from its central data mart.

We are still in the review stage for these PIAs and the quality of the risk analysis is not clear; however, we are aware of the increased reporting of PIAs to our Office.

## Recent Interactions between OPC PIA and CRA

In addition to the interaction between the OPC PIA group and the CRA on FATCA and sharing information with the Office of the Auditor General, our Office has had discussions on the following:



Commissariat  
à la protection de  
la vie privée du  
Canada

Office of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
Protected B	9 + Annex A

### Use of Employee SINs to Monitor Unauthorized Access

In an August 2016 conference call between the OPC's PIA group and the CRA, our Office was informed that the CRA is contemplating an initiative to monitor the SINs of employees' who have a need to access taxpayer records as part of their work. The CRA indicated that employees who improperly access their own accounts are likely to improperly access the accounts of other individuals thereafter. While the CRA has stated that a PIA has been completed for this initiative, we have yet to receive it. To date, we have only been provided with a supplementary document which gives a brief description of what is being contemplated.

s.23

While CRA asked for our views as part of a TB submission they were preparing to request an amendment to the Directive on SIN to specifically authorize the use of the SIN in this manner, we offered only preliminary concerns, stressing that we have not had the benefit of reviewing detailed information. Some of the preliminary concerns we raised included the fact that it is not clear how the use of a SIN to monitor employee access to information that is stored within the CRA's IT infrastructure is analogous to confirming identity to grant access to the infrastructure. Similarly, we noted it was unclear how there is a reasonable and direct connection (as required by the Directive on SIN) between the original purposes for the collection of the SIN – that is, to create a PRI, issue a T4, etc – and the monitoring of an employee's access to CRA records.

In short, we have been clear that, while we are supportive of the CRA's efforts to prevent unauthorized access to taxpayer information in line with recommendations made in our 2013 audit of the Agency, we were concerned that this use of the SIN is not in line with purposes outlined in the TBS Directive on SIN.

## **8. CRA Privacy Act Breaches and Investigations**

*NOTE: Investigation and breach statistics - in chart form - can be found in Annex A.*

### **Breaches**

From April 1, 2011, to the present, our Office has been notified of 132 breaches of personal information involving CRA. Of particular note is that between April 1, 2011 and September 7, 2016, the OPC received 94 reports from the CRA related to unauthorized access of personal information by CRA employees, over a third of which were reported in FY 2014/15 alone.

The increase in breach reporting for fiscal years 2013/14 and 2014/15 may be a result of due diligence activities undertaken by the CRA following the OPC's most recent audit, as well as the requirements of TBS policy with respect to mandatory reporting of material privacy breaches.<sup>3</sup>

<sup>3</sup> The Treasury Board Secretariat policy requiring reporting of material privacy breaches to both the TBS and the OPC came into effect in May 2014.



Commissariat  
à la protection de  
la vie privée du  
Canada

Office of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
Protected B	9 + Annex A

In recent years, the number of breaches reported to the OPC has trended downwards significantly, having decreased by over 47% in FY 2015/16 (21 incidents reported) and on track to fall another 33% this fiscal year.

The timeliness of the CRA's reporting of its privacy breaches is an ongoing concern, with notification of several unauthorized access breaches reaching our Office on average after 270 working days and occasionally up to two years or more after the occurrence, which can understandably negatively impact mitigation measures and timely notification of affected individuals.

PA Investigations has raised the issue with the CRA, but the Agency's officials have indicated that internal procedures require Security and Internal Affairs Directorate investigations be completed before the ATIP Office is informed of such privacy incidents.

### Heartbleed Bug

- In April 2014, an intruder took advantage of the Heartbleed vulnerability (a security weakness found in certain software that secure websites use to encrypt user names, passwords and financial information) and accessed the Social Insurance Numbers (SIN) and additional personal information of some 900 taxpayers.
- While the CRA was the victim of the intrusion, the Agency was able to respond swiftly and decisively. Its measures included shutting down its EFILE system as the income tax filing deadline neared, stepping-up monitoring of its IT systems to detect intrusions, sending a registered letter to each of the individuals affected by the intrusion, and providing a dedicated 1-800 number they could call.
- The CRA also provided those affected with access to credit protection services, and flagged their CRA accounts to monitor for any unauthorized activity. As an additional step, the CRA informed Employment and Social Development Canada of the SINs that had been compromised so it could monitor its accounts as well.

### **Investigations**

Over the last decade, the CRA has featured in the top ten institutions about which our Office has received complaints under the *Privacy Act*, with the exception of 2008-09.

In the last five fiscal years, the CRA has averaged fifth overall among federal institutions in the number of privacy complaints received.

On average, over the last five cycles, the OPC has accepted 56% of access and delay type complaints and 44% of privacy (sections 4 to 8) type complaints against the Agency, fully one quarter of which were closed through the early resolution process.

We still see high volumes of complaints involving the CRA this fiscal year.

Our Office had 2 recent prominent investigations involving the CRA. Both of these have been issued in our annual reports, these were:





Commissariat  
à la protection de  
la vie privée du  
Canada

Office of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
Protected B	9 + Annex A

- Adequate measures to ensure personal information is not moved to U.S.<sup>4</sup>
- Complaints against the Canada Revenue Agency (CRA) in relation to a privacy breach wherein the personal information of approximately 1,000 individuals was inadvertently mailed to the Canadian Broadcasting Corporation (CBC).<sup>5</sup>
  - Our investigation confirmed the information was inadvertently sent to the CBC. Following our investigation, we concluded that the complaints against the CRA were well-founded. Given that the CRA took immediate action to strengthen its personal information handling practices, we were satisfied that no further action was required by our Office.

## 9. Other Issues

### Anti-Money Laundering

Our Office is aware that with respect to the anti-money laundering/anti-terrorist financing (AML/ATF), there have been a number of issues raised in relation to tax authorities:

- In 2015 the OECD issued a report entitled "*Improving Co-operation Between Tax and Anti-Money Laundering Authorities*".<sup>6</sup> Among other issues, the report commented upon the merits of expanding the role of tax authorities in submitting and receiving AML/ATF suspicious transaction reports.
- As well, the Financial Action Task Force (FATF) in its 2016 mutual evaluation of Canada,<sup>7</sup> suggested FINTRAC should have access to information collected by the CRA for the purposes of its analysis of suspicious transaction reports.

### OECD Common Reporting Standard (CRS)

Our Office is aware that the OECD CRS is modeled after FATCA and meant to serve as an automatic sharing of certain taxpayer information among partner countries that have signed the information sharing agreement. We are aware that CRS implementing legislation has been introduced in the latest Budget Bill under Part XIX.

Financial institutions in Canada are expected to begin these obligations in July 1, 2017. As of that date, Canadian financial institutions would be required to have procedures in place to identify accounts held by non-residents and to report the required information to the CRA, who in turn will forward reports to tax authorities in partner countries. The first exchange by the CRA is expected to take place in 2018.

- Unlike FATCA, reporting on accounts is not based on citizenship, but on tax residency. As well, there is no threshold limit, so all accounts where there is an indicia of tax residency with a partner country will be reported by the CRA.

<sup>4</sup> Canada Revenue Agency takes adequate measures to ensure personal information not moved to U.S. – Investigation involving Canada Revenue Agency and a contract it had with Mobilshred Inc

<sup>5</sup> Canada Revenue Agency and the Canadian Broadcasting Corporation (CRA)

<sup>6</sup> OECD, "Improving Co-operation Between tax and Anti-Money Laundering Authorities" September 18, 2015.

<sup>7</sup> Financial Action Task Force, "2016 Mutual Evaluation Report of Canada" September 2016.



Commissariat  
à la protection de  
la vie privée du  
Canada

Office of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
Protected B	9 + Annex A

The CRA has information on its website on the CRS and has noted that: *“It is not proposed that financial institutions automatically notify their account holders about reporting to the Canada Revenue Agency in connection with the Common Reporting Standard. However, financial institutions will be expected, upon request, to inform account holders whether their personal information has been reported”*.

Previously, the CRA has advised that a PIA on this initiative will be sent to our Office. The FATCA PIA also notes that it will be updated to cover the CRS.

- We have not received detailed briefings from the CRA or Finance Canada on the CRS and have not been advised when we can expect the PIA. Our Office is currently preparing a briefing note on the Bill C-29, including the CRS provisions.

### Tax Avoidance and Evasion

Following news of the Panama Papers, the House of Commons Standing Committee on Finance undertook a study of CRA's efforts to combat tax avoidance and evasion. The study began in May 2016 and is still on-going. In the CRA's appearances before the Committee, it has commented on its:

- information sharing activities,
- international activities (including its OECD partnerships), and
- updated initiatives to combat tax evasion and offshore tax avoidance.

We are also aware that the CRA had undertaken a series of PIAs on offshore tax evasion in 2013, which they had discussed with our Office.

**DISTRIBUTION:** The Commissioner, LSPRTA, DG A&R, DG PIPEDA, DG PA, DG Communications, Director Toronto Office

**CONSULTATIONS:** Jean Plamondon, Prosper Béral, Chris Prince, Lara Ives, Lindsay Scotton, Lacey Batalov, and Mike Fagan

### **APPROBATION / APPROVAL:**

Rédigé par / Prepared by Arun Bauri	Date October 25 <sup>th</sup> 2016	Revisions
Approuvé par / Approved by Barbara Bucknell <i>Directrice, Politiques et recherche / Director, Policy and Research</i>	Date	



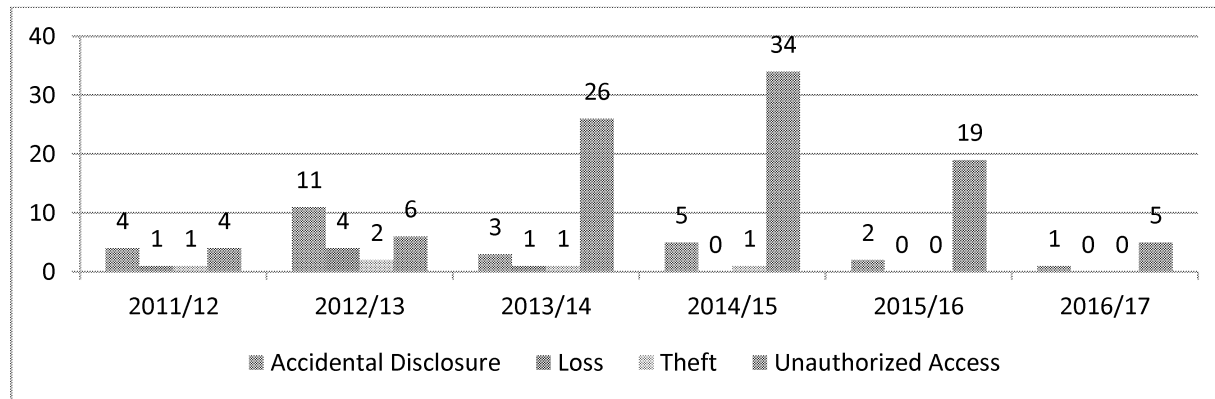
Commissariat  
à la protection de  
la vie privée du  
Canada

Office of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
Protected B	9 + Annex A

## Annex A

### Privacy Breaches reported by the CRA (Last Five Fiscal Years and Current FY to date)



### Complaints accepted against the CRA (Last Five Fiscal Years)

	2011-12	2012-13	2013-14	2014-15	2015-16	Total	Five-Year Average
Complaints accepted	65	78	61	106	86	396	79
Rank in Top 10	4	7	6	3	4		5

### Complaint types (Last Five Fiscal Years)

	2011-12	2012-13	2013-14	2014-15	2015-16	Total	Five-Year Average	Percent of total
Access	24	41	23	22	17	127	25	32%
Time Limits	23	21	13	23	15	95	19	24%
Privacy ("4 to 8s")	18	16	25	61	54	174	35	44%
<b>Total</b>	<b>65</b>	<b>78</b>	<b>61</b>	<b>106</b>	<b>86</b>	<b>396</b>	<b>79</b>	<b>100%</b>

### Dispositions of complaints closed (Last Five Fiscal Years)

	2011-12	2012-13	2013-14	2014-15	2015-16
Well-founded	17	20	5	8	19
Well-founded resolved	1	5	1	5	5
Not well-founded	17	21	20	13	10
Settled	3	3	1	0	0
Resolved	0	2	1	8	1
Discontinued	16	1	5	5	57
No jurisdiction	0	0	1	0	0
Early resolution	12	15	18	33	12

NOTE TO COMMISSIONER

From: Valerie Lawton c.c. Anne-Marie Hayden, Brent Homan  
Date: September 12, 2016  
Subject: ALM Media Analysis

---

Commissioner,

As you know, we initiated a contract with a firm, MediaMiser, to prepare an analysis of the media coverage of the Ashley Madison data breach investigation.

Please see enclosed a copy of the report, for your review/feedback.

Of note, the company has estimated that the coverage reached more than 128 million people around the globe, and that the vast majority of stories picked up our key messages.

Valerie

---

I am satisfied with the analysis

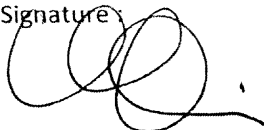
I have comments/wish to propose changes

I have questions / wish to discuss

→ How successful were we  
with our message that  
this was not an isolated  
case?

Comments:

Signature:



12/9/16



Commissariat  
à la protection de  
la vie privée du Canada

Office of the  
Privacy Commissioner  
of Canada

# Ashley Madison Data Breach Investigation

## Media Coverage Report

August 23 – 31, 2016

presented by  MediaMiser



Commissariat  
à la protection de  
la vie privée du Canada

Office of the  
Privacy Commissioner  
of Canada

# Table of Contents

- Executive Summary.....3
- Methodology.....4
- Coverage Trend.....5
- Key Messages.....6
- Spokespeople.....8
- Sentiment.....9
- Top Authors.....10
- Top Outlets.....11
- Media Type & Regions.....12
- Conclusion.....13

Commissariat  
à la protection de  
la vie privée du CanadaOffice of the  
Privacy Commissioner  
of Canada

# Executive Summary

## Background

The Office of the Privacy Commissioner of Canada and the Office of the Australian Information Commissioner jointly conducted an investigation into the breach of Toronto-based Avid Life Media Inc's (henceforth referred to as Ashley Madison) computer network, and found numerous violations of privacy laws in both countries. A news release detailing the key findings was released on August 23, 2016. This report analyzes the media coverage garnered on the released report and the key messages from the report that were highlighted in the media.

## Coverage Summary

Total Coverage	August 23 Coverage	August 24 – 31 Coverage
Total Articles: 788	Articles: 539	Articles: 249
Total Reach: 128,135,086	Circulation: 94,915,526	Circulation: 33,219,560

## Key Highlights

- The report received a strong pick-up in the media, with all major wire services, including Associated Press, Canadian Press, Postmedia, Agence France-Presse (AFP), Australian Associated Press (AAP), Reuters, DowJones, and IDG service writing feature-length pieces on the report and highlighting many of the key messages.
- Coverage came across all major media, including key top tier publications such as *The Globe and Mail*, *National Post*, *Toronto Star*, *The New York Times*, *The Washington Post*, *Sydney Morning Herald*, *The Age*, *BBC*, and *The Daily Telegraph*, among others.
- The success of the release was further evidenced in the extensive coverage of the key messages in media. More than two-thirds of coverage highlighted three or more messages. The majority of the coverage picked up the exact language of the key messages communicated via the press release to the media, a not-so common occurrence.
- The report was also well covered on TV and radio media, with *CBC* providing in-depth footage including comments from privacy commissioner, Daniel Therrien. *AM 980 Vancouver (CKNW)* also featured the full interview with Daniel Therrien. *CTV* also ran the news story on its national and regional news networks. A few pick-ups on U.S. stations were also noted.
- Ashley Madison's lack of adequate security safeguards, use of fake security trustmark, and entrance into a compliance agreement/agreed to follow the recommendations, were the three most communicated key messages.
- Overall, Daniel Therrien was the most widely quoted spokesperson. His quotes appeared in close to 50 per cent of the articles. Timothy Pilgrim's quote was more prevalent in the Australian media coverage.



Commissariat  
à la protection de  
la vie privée du Canada

Office of the  
Privacy Commissioner  
of Canada

# Methodology

## Objective

To analyze media coverage generated on the investigative report jointly conducted by Office of the Privacy Commissioner of Canada and the Office of the Australian Information Commissioner into the breach of Toronto-based Ashley Madison's computer network.

## Content

Print – All Canadian print media and select print content globally available through MediaMiser's print module was monitored.

Online – More than 100,000 online sites and blogs globally were monitored towards the coverage.

Broadcast – In-depth Canadian and U.S. broadcast library and select international broadcast radio and TV was monitored.

## Analysis

- All coverage was analyzed using MediaMiser proprietary technology for metrics such as coverage trend, top authors, media outlet & type, and spokespeople.
- The identified key messages were manually tagged and analyzed. The seven identified key messages analyzed were:
  - Lack of adequate security safeguards and their implementation
  - Ashley Madison violated numerous privacy laws in Canada and Australia
  - Use of phony security trustmark on Ashley Madison's website
  - Lessons learned for other businesses with regards to privacy
  - Proper retention/deletion of user data
  - Accuracy of user emails
  - Compliance agreement entered into by Ashley Madison
- All coverage was also toned as either positive, neutral, or negative. Articles re-enforcing one or more key messages were toned as positive; absence of any key message was toned as negative. Any negative critique of report process, rationale, or miscommunication of key messages was toned as negative. For this report, no negative coverage was noted.

## Key Definition

**Reach** – Circulation value for print publications, audience reach for TV and radio, and Unique Visitor Value for online sites were considered towards the reach calculation of the coverage.





Commissariat  
à la protection de  
la vie privée du Canada

Office of the  
Privacy Commissioner  
of Canada

# Coverage Trend

## Coverage Summary

Total Articles: 788

Total Reach: 128,135,086

## August 23 Coverage

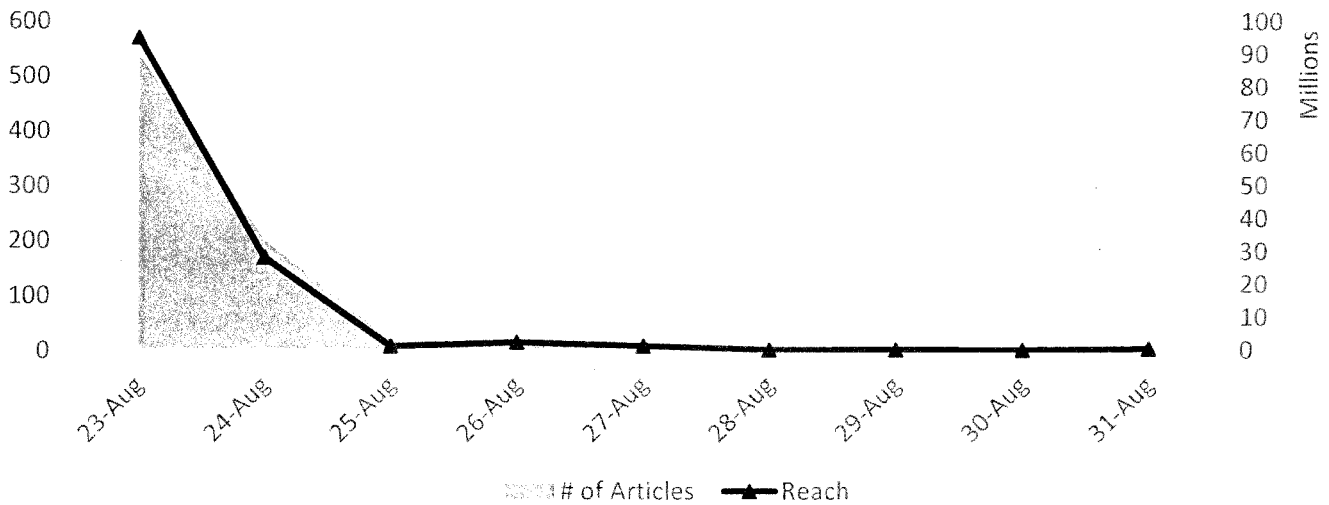
Articles: 539

Circulation: 94,915,526

## August 24 – 31 Coverage

Articles: 249

Circulation: 33,219,560



- Media coverage of the Privacy Commissioner’s investigation of Ashley Madison’s data breach garnered a total of 788 articles, with a reach of more than 128 million.
- The report and its findings were widely covered in the media, with all major wire services writing feature-length articles on the report. The stories were published in all top outlets in Canada, the U.S., and Australia, and even the UK. Some notable publications included *The Globe and Mail*, *The New York Times*, *The Daily Telegraph*, *BBC*, and *Sydney Morning Herald*.
- The success of the coverage was more directly evidenced through the extensive communication of the key messages, with more than two-thirds of the coverage reporting on at least three key messages.
- Ashley Madison’s lack of adequate security safeguards, use of phony trustmark, and the fact that the company has agreed to follow the recommendations or entered into a compliance agreement were the three most communicated key messages that emerged in the media. What is also noteworthy is that the media used exact language from the press release in their write-ups, highlighting the success of the messaging process by the Privacy Commissioner’s office.



Commissariat  
à la protection de  
la vie privée du Canada

Office of the  
Privacy Commissioner  
of Canada

# Key Messages

## Top Key Messages



The 788 articles that were gathered on the report were analyzed for the seven key messages; they are highlighted by volume and reach in the above bar chart.

The news release noted not only an extensive pick-up of the key messages but also targeted messaging, as evidenced in the coverage results below and the following page.

- More than 95 per cent of the coverage focused exclusively on the report and its findings, highlighting one or more of the key messages.
- Ninety-four per cent of the articles clearly enunciated that Ashley Madison did not have adequate security safeguards and implementation processes in place.
- Almost all the coverage reprinted the exact language of the press release, thereby minimizing any miscommunication of key messages and highlighting the preciseness of the key message communication undertaken by the Privacy Commissioner's office.
- There were two syndicated articles that did not highlight any specific key message but still noted that the OPC has released the security findings on Ashley Madison. One such story was regarding the *BBC* documentary on Ashley Madison that was being aired the same week. The timing of the documentary coinciding with the report release helped the report get significant mileage in the UK media as well.

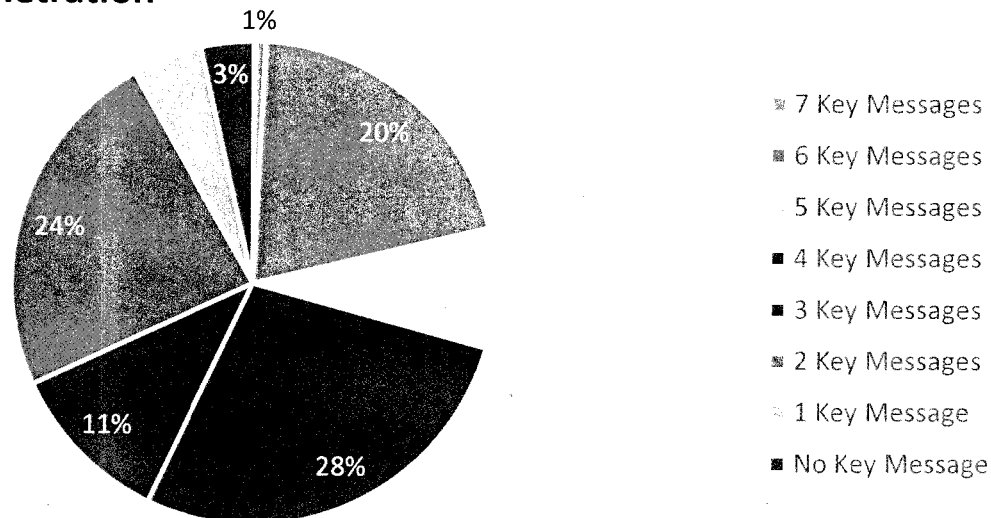


Commissariat  
à la protection de  
la vie privée du Canada

Office of the  
Privacy Commissioner  
of Canada

# Key Messages

## Key Message Penetration



The above pie chart showcases percentage of articles by the number of key messages featured in these articles.

- The strong media penetration of the key messages was evidenced by the fact that more than two-thirds of the coverage spoke of at least three key messages.
- Several prominent publications in Canada, the U.S., the UK, and Australia covered the news, with articles highlighting several key messages. Some notable ones are:
  - Canada – *The Globe and Mail*, *National Post*, *Toronto Star*, *CBC.ca*, *Vancouver Sun*;
  - USA – *The New York Times*, *The Washington Post*, *NBC*, *San Francisco Chronicle*;
  - Australia – *Sydney Morning Herald*, *The Age*, *Brisbane Times*;
  - Europe – *The Daily Telegraph*, *The Guardian*, *France24*
- *CBC TV*, on its national news program ‘*CBC News Network with Heather Hiscox*’, aired a piece on the report, highlighting all the key findings of the report, and also showed privacy commissioner Daniel Therrien’s quote. *CBC* also did a radio piece that touched upon five of the key messages.
- *CTV National News* also repeatedly aired the news, and also noted syndication of this news across several regional stations.

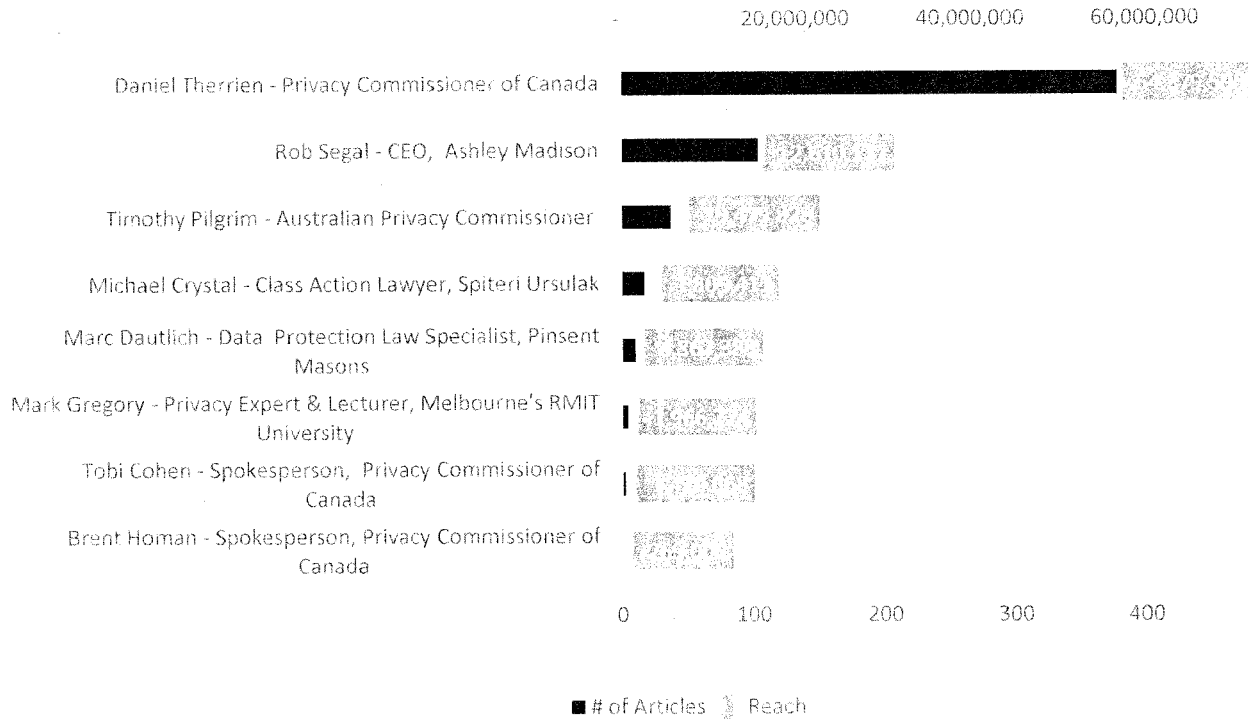


Commissariat  
à la protection de  
la vie privée du Canada

Office of the  
Privacy Commissioner  
of Canada

# Spokespeople

## Top Spokespeople



## Most quoted quotes by top Spokespeople

"Where data is highly sensitive and attractive to criminals, the risk is even greater. Handling huge amounts of this kind of personal information without a comprehensive information security plan is unacceptable. This is an important lesson all organizations can draw from the investigation."

*Daniel Therrien, Privacy Commissioner of Canada*

The breach comes as a stark reminder for consumers to be more informed about the business they are entrusting their information to. "Be clear about what you are providing, the value you are getting in exchange, and understand that no organisation is 'breach-proof.'"

*Timothy Pilgrim, Australian Privacy Commissioner*

"The company (Ashley Madison) continues to make significant, ongoing investments in privacy and security to address the constantly evolving threats facing online businesses. These investments are the cornerstone of rebuilding consumer trust over the long term."

*Rob Segal, CEO, Ashley Madison*

"This type of document sends a strong message. These corporate entities that are making a good deal of money from our information have a matching responsibility to protect it."

*Michael Crystal, Class Action Lawyer at Spiteri & Ursulak*

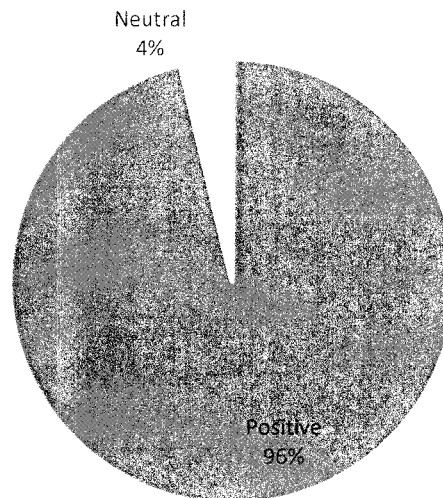


Commissariat  
à la protection de  
la vie privée du Canada

Office of the  
Privacy Commissioner  
of Canada

Sentiment

## Coverage Sentiment



- The report was very positively received by the media, with over 95 per cent of the coverage being noted as positive.
- Media coverage primarily took the key points from the report, including highlighting the lax security standards at Ashley Madison, poor implementation, phony trustmark, and eventually the message regarding the company entering into compliance agreement.
- There was no negative coverage noted. Most articles focused on the key messages that were being communicated, and there was no critique of the process or rationale for the investigation.
- Less than four per cent of the coverage was noted as neutral. These were articles that focused either on the subject of privacy in general or other aspects of Ashley Madison coverage, and made mention of the report only in passing or as an indirect reference.

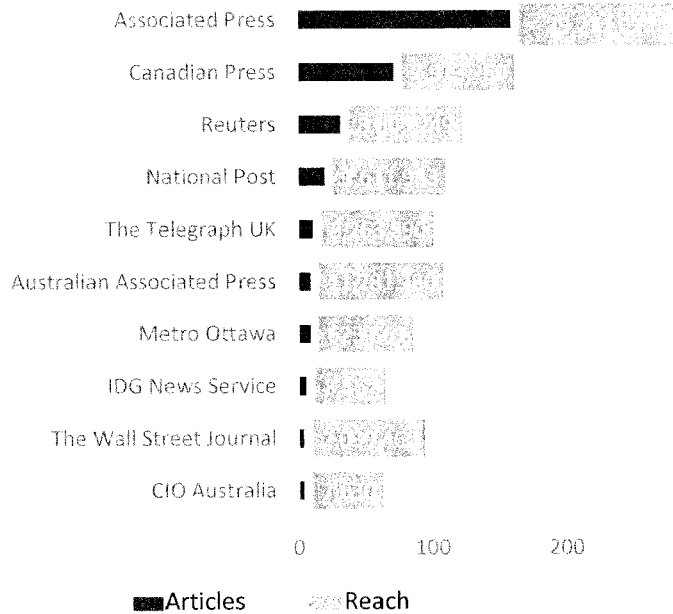


Commissariat  
à la protection de  
la vie privée du Canada

Office of the  
Privacy Commissioner  
of Canada

# Top Authors

## Top Syndicated Publications



- Associated Press, Canadian Press, and Reuters were the top three syndicated outlets.
- Of the top sources, three were Canadian, while three were Australian.
- Though Wall Street Journal article was only picked up in four other sources, coverage-reach wise it noted significantly higher reach compared to few others in the top ten list.

## Top Syndicated Articles

Publication	Total Articles	Total Circulation
<u>"Cheating site had inadequate security, privacy officials say"</u> in Associated Press	160	29,211,022
<u>"Ashley Madison had inadequate security safeguards, privacy officials say"</u> in Canadian Press	72	2,913,250
<u>"Ashley Madison parent broke Canada, Australia privacy laws"</u> in Reuters	32	8,605,249
<u>"Cheater site criticised for safety standards"</u> in <i>The Toowoomba Chronicle</i>	22	837,241
<u>"Canada, Australia privacy watchdogs find Ashley Madison lacked security"</u> in <i>Agence France-Presse</i>	20	6,077,819
<u>"Privacy probe finds lax security, deceptive practices at Ashley Madison"</u> in <i>National Post</i>	20	1,611,983
<u>"Sex, lies and fembots: one year on from the hack, what really happened at Ashley Madison?"</u> in <i>The Telegraph</i>	11	3,263,590
<u>"International report into Ashley Madison hack 'highly critical' of site's privacy"</u> in <i>Australian Associated Press</i>	9	11,281,780
<u>"La sécurité d'Ashley Madison était "inadéquate" selon le Canada et l'Australie"</u> in <i>Agence France-Presse</i>	9	1,054,593
<u>"Ashley Madison slated over security"</u> in <i>BBC News</i> (on Aug. 23)	8	4,771,241

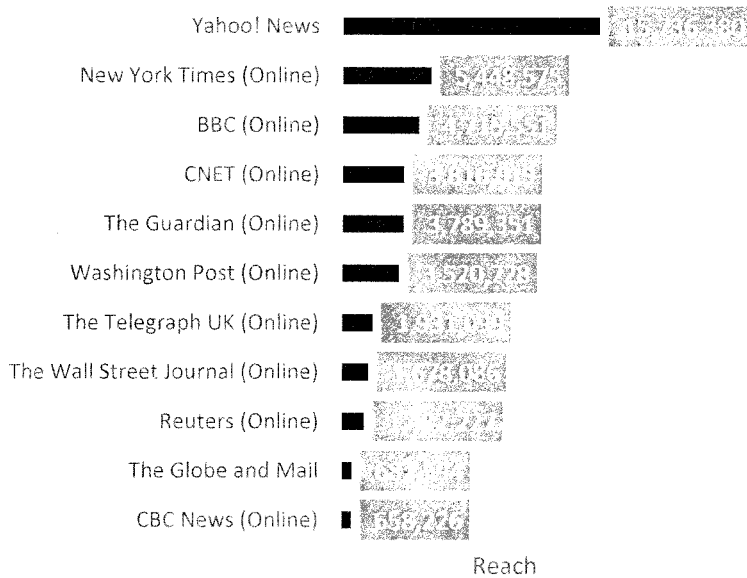


Commissariat  
à la protection de  
la vie privée du Canada

Office of the  
Privacy Commissioner  
of Canada

# Top Outlets

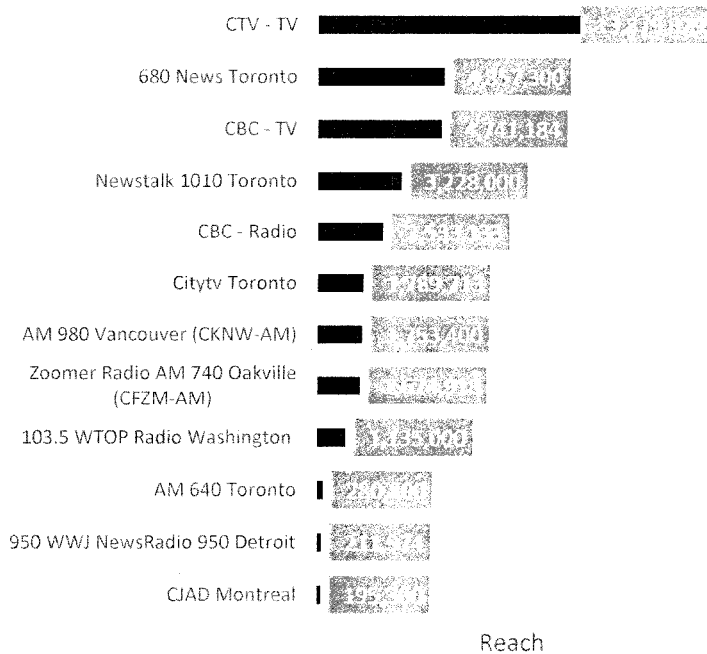
## Top Print and Online Outlets



Top outlets noted on the adjacent graphs are ranked by highest reach.

- The report received widespread coverage across the globe in most leading papers. Some other notable publications not shown in the graph are *Sydney Morning Herald*, *Australian Age*, *Brisbane Times*, and *National Post*, among others.
- Yahoo! News* was the top outlet, as it published Canadian and international wire stories, given its international media presence. Articles from Lexology were all posted in days following the initial announcement. Lawyers posted blog posts, analyzing the findings of the report from a legal perspective.

## Top Broadcast Outlets



- Overall, the Privacy Commissioner's report was well covered in both television and radio across the country. Television and radio coverage accounted for close to 40 per cent of all coverage.
- Both *CTV* and *CBC* TV and radio coverage of the report was widely syndicated on stations across the country. While *CTV* did a minute-long piece, *CBC's* report was more in-depth, highlighting all the key findings while also including a comment from Daniel Therrien.
- Newstalk 1010* also thoroughly covered the investigation's findings, drawing on expert analysis and spokespeople's comments. Brent Homan, director of the Privacy Commissioner's office, was quoted in this coverage. *Newstalk* also included comments from Michael Crystal, class action lawyer, for his take on the report.

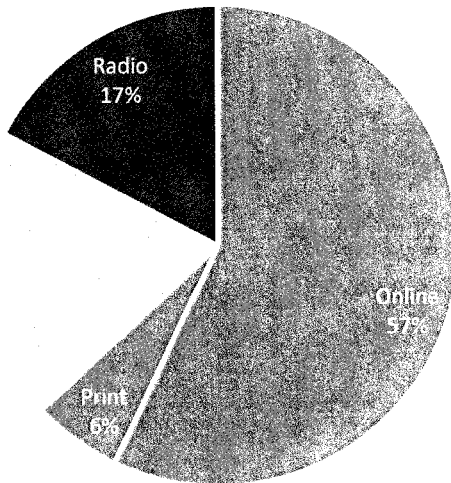


Commissariat  
à la protection de  
la vie privée du Canada

Office of the  
Privacy Commissioner  
of Canada

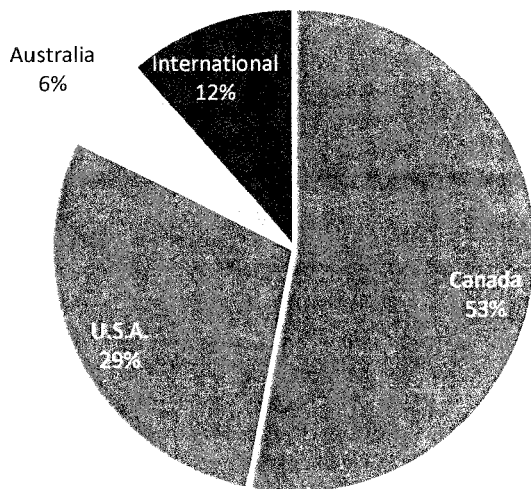
# Media Type & Region

## Media Outlet Type



- Online comprised more than 50 per cent of the total coverage. The majority of the online articles were syndications of the Canadian Press and Associated Press articles. However, during the days following the announcement, online coverage continued, as blog posts and articles examining the legal implications of the investigation's findings appeared, especially lessons learned from the report for organizations in general.
- Television coverage accounted for one-fifth of total coverage, as *CTV* and *CBC* covered the story widely across their national and regional networks. The repeated airings of the radio clips further contributed to the total volume of broadcast coverage.
- While television coverage was slightly higher than radio coverage, radio stations provided more in-depth analyses of the report. For example, *Newstalk 1010* interviewed lawyer Michael Crystal, and *AM 980 Vancouver* aired its full interview with Privacy Commissioner Daniel Therrien.

## Top Regions



- The majority of media coverage came from Canada, as Canadian Press's English and French wire stories were picked up in print and online by many publications across the country, both large and small.
- The second region was the U.S., as many outlets also ran wire stories. The top wire story came from Associated Press, and was heavily syndicated across regional and national papers, such as *The New York Times* (Online), *The Miami Herald* (Online), and *Seattle Times* (Online). A select few U.S. TV stations also mentioned the report.
- Coverage from Australia accounted for 6 per cent of the total.
- Other international outlets (outside of Canada, the U.S., and Australia) drove coverage with 12 per cent of the total.





Commissariat  
à la protection de  
la vie privée du Canada

Office of the  
Privacy Commissioner  
of Canada

## Conclusion

The report findings on the Ashley Madison security breach investigation, jointly conducted by the Office of the Privacy Commissioner of Canada (OPC) and the Office of the Australian Information Commissioner, received significant traction in the media. Overall, the release was very successful in communicating the key findings/messages through the media to the general public at large. This is evidenced in the below results that were garnered from the media analysis:

- Almost all major wires wrote a feature-length article on the report findings.
- Top tier publications in Canada, the U.S, the UK, and Australia prominently published stories on the report.
- Besides successful print and online pick-up, the report also noted significant coverage in Canadian broadcast media, with many leading networks, i.e. *CBC*, *CTV*, *Global*, *CityTV*, and prominent radio stations such as *680 News*, *AM 980 Vancouver*, *CFRA* etc., providing in-depth footage on this news. The news was also picked up on some regional *ABC* and *NBC* stations in the U.S.
- More than two-thirds of the coverage clearly highlighted three or more key messages, while more than 97 per cent highlighted at least one.
- The language used in the news coverage was a direct pick-up from the press release, highlighting the clear and precise messaging put forth by OPC's communication team.
- Daniel Therrien's quote was mentioned in over 350 articles, including in *CBC TV's* broadcast feature, where the network included his exact quote, which was read by the host. This again highlights the success of the targeted messaging to the media.

NOTE TO COMMISSIONER

From Valerie Lawton c.c. Anne-Marie Hayden, Daphne Guerrero  
Date November 4, 2016  
**Subject Plan for the creation and management of an OPC Facebook Page**

---

Commissioner,

Following your agreement on the recommendation to create a Facebook Page to further our public outreach efforts, we have updated the strategy outlining how the OPC would use Facebook. You will recall that you had reviewed and approved an earlier version of this strategy in August, which had been reviewed by both the Office's CPO and discussed with the Privacy Accountability Working Group (PAWG).

The updated strategy now includes a section outlining the OPC's overall approach to developing and managing the OPC's Facebook Pages. This new section contains:

- A proposed approach to sharing and engaging
- Foundational elements to launch the page (OPC Facebook Comment Policy, OPC Facebook Privacy Notice, Posting guidelines / Service standards )
- Compliance with Government of Canada policies and guidelines (Identity, Official Languages, Accessibility, Publishing, Account configuration and compliance)
- Development of the Facebook Page (Development and branding, Account Verification)
- Ongoing management (Posting, Approval process, Daily management of Facebook page)
- Evaluation

We are seeking your approval for the overall approach and the following documents included in the strategy: OPC Facebook Comment Policy and OPC Facebook Privacy Notice.

Also attached for your approval is a proposed launch strategy for the Facebook Pages. We are targeting a launch on December 5.

We would propose to conduct a demonstration of the Page for you at an upcoming bilat.

---

**Revisions and/or approval**

- I approve this strategy and launch plan.
- I have revisions and wish to see a new version of the strategy and launch plan.
- I have questions/concerns regarding this file and wish to discuss.

Comments :

Signature :

## OPC Facebook Page Strategy

### Table of Contents

Background.....	1
Objectives.....	2
Additionally: .....	2
Consultations.....	2
Considerations.....	2
Overall approach .....	5
Communicating and Engaging.....	6
Foundational elements .....	6
Compliance with Government of Canada policies and guidelines.....	9
Development of the Facebook Page .....	10
Launch .....	11
Ongoing management.....	11
Evaluation.....	12
Critical path .....	14
Annex A – Examples of posts.....	15

### Background

The OPC will be establishing a Page on Facebook for the purposes of communicating with Canadians as part of the Office's outreach efforts. In particular, the page will focus on communicating with parents of children and young people, in support of our youth outreach strategy.

This was discussed at HIF in November 2015, and approved by the Commissioner in March 2016.

According to Facebook, Pages "are for businesses, brands and organizations to share their stories and connect with people.... People who like your Page and their friends can get updates in News Feed."<sup>1</sup> Pages can only be created and managed by an official representative of the business or organization.

Research suggests that Canadians are avid social media users, with Facebook as the most popular social network among Canadians. A Forum Research survey conducted in 2015 found that 59% of respondents had Facebook accounts, compared to 30% of Canadian respondents on LinkedIn, 25% on Twitter and 16% on Instagram. (According to Facebook's own research, 14 million Canadians check their Facebook

<sup>1</sup> *What is a Facebook Page?*, Facebook Help Centre, <https://www.facebook.com/help/174987089221178>

newsfeed every day.) Additionally, a study by the U.S.-based Pew Research Center study suggests that a large number of parents (66%) find parenting advice while looking at social media content.

## Objectives

- To establish an OPC Facebook page devoted to and focused on communicating to Canadians in general, and in particular, communicating directly to parents with information on privacy issues and risks, and tips and strategies to mitigate those risks.

## Additionally:

- to ensure that the OPC brand is properly reflected on our Facebook presence; and
- to ensure that our use of Facebook is compliant with our own internal privacy policies, the *Privacy Act* and relevant TBS guidance regarding federal government use of social media, and that our privacy practices with respect to our use of Facebook is consistent with the advice we have given other organizations.

## Consultations

Following a discussion at HIF on the potential of expanding the Office's use of social media (beyond its blog, Twitter, YouTube and LinkedIn accounts) to include Facebook, HIF recommended that Communications consult with two DPAs currently using Facebook to better understand their considerations before establishing a presence on Facebook, specifically as it relates to the privacy of Facebook users who choose to follow these DPAs on Facebook, and any perceived conflicts of interest.

The OPC consulted with the UK's Information Commissioners' Office (ICO) and the Office of the Australian Information Commissioner (OAIC). Additionally, Policy & Research (P&R) assessed the risks, from a policy perspective, of our Office establishing a presence on Facebook.

## Considerations

### Perceived conflict of interest

There is the risk of a perceived conflict of interest, given that we have investigated Facebook's privacy practices in the past and could receive complaints where Facebook is named as the respondent. In its risk assessment, P&R determined that the risk that the Office could receive a complaint related to Facebook Pages is minimal as they consider such a complaint unlikely. As well, P&R concluded that there is minimal risk that the OPC might be seen to be endorsing a non-privacy compliant Facebook feature. (The risk assessment is contained in Officium document 7777-6-123918.)

In the consultations with the ICO and OAIC, both organizations concluded that there was minimal risk that their respective organizations might be seen to be endorsing a non-privacy compliant Facebook feature through their use of a Facebook page. However, both organizations drew the line at partnering

with Facebook in other ways – for example, like the OPC, who was also approached, both chose not to partner with Facebook to create a Data Privacy Day video that would be promoted on Facebook.

Facebook has been the subject of previous OPC investigations. Should Facebook become the subject of another investigation, Communications would consult with LSPRTA and PIPEDA Investigations to review this strategy and assess whether our use of Facebook as an organization would require any changes.

#### Privacy on social media:

Given our role, we must be cautious in our use of a new social media channel. This strategy is meant to address concerns with respect to user privacy and the OPC's use of Facebook. The approach was reviewed by the OPC's CPO, and discussed with the Office's Privacy Accountability Working Group (PAWG). It will be reviewed and approved by the Commissioner before the Page is launched.

The OPC has a formal process in place to determine if a PIA is necessary before launching a new project. If personal information is being collected, a PIA questionnaire must be completed. The questionnaire helps inform the CPO and PAWG in their consideration of whether a PIA is required. However, in this case, the OPC has confirmed with its CPO that, as with our approach to LinkedIn, a PIA is not required as the OPC, in its use of Facebook, will not be actively collecting any personal information, as defined in the *Privacy Act*, from its Facebook page. Communications has reviewed the questions in the PIA questionnaire and can confirm that it will not be collecting or using personal information in any of the ways identified in the questionnaire.

In our consultations with the ICO and the OAIC, they indicated they did not record or retain data about the people who follow/like their Facebook pages. Additional information on how the OPC would collect and use information via Facebook is in the section entitled *Collection and Use of Information Gathered on Facebook* in this document.

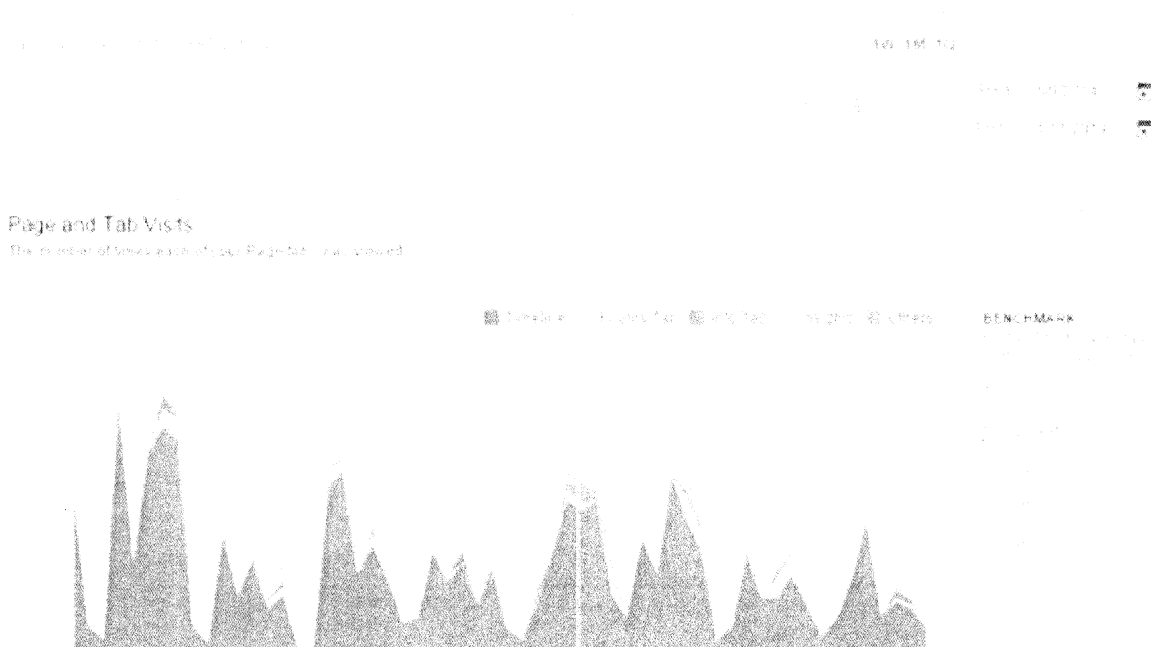
As part of the OPC's implementation plan, an OPC Facebook Privacy Notice would be drafted by our Office, explaining the OPC's collection and use of information gathered on Facebook, and a link to this notice would appear prominently on our page. Moreover, this notice would explain the third-party nature of the Facebook platform, note that Facebook users are bound by Facebook's Terms of Service and Privacy Policy, and encourage users to read the Terms of Service and Privacy Policy. For an example of what this notice could look like, please see our [LinkedIn](#), [Twitter](#) and [YouTube](#) Privacy Notices. Legal Services has reviewed these Privacy Notices and had no concerns. They will review the draft Facebook Privacy Notice and Comment Policy (discussed below) before the launch of the Page.

In its assessment, P&R also identified the risk that visitors to our Facebook page could post personal information (their own or someone else's) on our page. To mitigate this risk, P&R has recommended that we review all comments made to our page before posting, and delete or remove comments from our Page as appropriate. Facebook has the functionality to allow page administrators to do this. (However, we would note that [Facebook's privacy policy](#) indicates that these comments and/or information about these comments) are collected and retained, even after being removed from a page. We employ this same practice for comments readers make on our blog, and this practice would be outlined in our Facebook Comment Policy, explained further below in this document. A reminder about not posting personal information will also appear in the Privacy Notice.

### *Collection and Use of Information Gathered on Facebook*

The OPC will not collect, record or retain any personal information, as defined in the *Privacy Act*, on Facebook.

Facebook provides aggregate data on page activity – e.g. number of likes, page visits and reach. (See screenshot below.) This data does not identify individual users. The OPC would use this aggregated information to evaluate and improve its use of Facebook as an outreach tool.



Comments made by Facebook users on our page or in response to our posts would be visible to other Facebook users. The amount of information that can be viewed about any Facebook user would depend on the privacy settings of that follower's account. This information will not be recorded or retained for any purpose. This will be made clear in our Privacy Notice, as has been done in the Privacy Notices for YouTube, LinkedIn and Twitter.

Staff with "administrator access" to the OPC's Facebook page will be limited to the Manager of Public Education and Outreach, the Director General of Communications, and one other communications advisor (as a back-up).

As per the OPC's [Privacy Notice](#), should the OPC become aware of comments that violate Canadian law, they will be deleted and such comments may be disclosed *to law enforcement authorities*.

#### Social media use policies and guidelines:

Treasury Board of Canada Secretariat has recently released a new Policy on Communications and Federal Identity, a supporting Directive on the Management of Communications and a Policy on Acceptable Network and Device Use. While the OPC is not subject to some parts of these policies and key portions of the directive, all Government of Canada institutions are encouraged to adopt the practices outlined in the policies and supporting directives, as appropriate. TBS' Directive on the Management of Communications encourages clear accountability for the management and coordination of departmental Web 2.0 initiatives and the development of strategies, plans and protocols for personnel on the use of Web 2.0. The OPC also has developed its own Acceptable Use of Electronic Networks Policy which defines the requirements for secure, ethical and appropriate use of OPC's electronic networks for business purposes.

ESDC and TBS have developed a draft Standard Privacy Impact Assessment (S-PIA) to determine the overall privacy risks associated with the use of official federal government social media accounts on a number of different platforms, including Facebook, and provide recommendations to mitigate these risks. The document has not yet been finalized nor has the OPC (Audit and Review) received it for review. As well, A&R has questioned whether the S-PIA should cover the use of so many different platforms. Note that the S-PIA covers a broad range of *activities* that departments could undertake using social media, including activities where, *unlike* the OPC's proposed use of one feature on Facebook, personal information may be collected. A&R will engage Policy and Research, as well as Communications, as appropriate, with respect to either further discussions relating to the S-PIA or other relevant PIAs on the use of social media by the GOC.

#### Reaching *other* audiences via Facebook:

At the moment, small businesses or other key OPC target audiences would not be viewed as the primary audience for use of this tool, as small businesses tend to use the Facebook platform to reach customers (as opposed to using the platform as a source for information about running a business). In the future, we could decide to broaden our use of Facebook to reach other audiences. Should this be contemplated, Communications will consult with others as appropriate.

#### Day-to-day management of the OPC Facebook page:

The OPC is currently active on LinkedIn and Twitter, and also has a YouTube account. Day-to-day management of the OPC Facebook page would be coordinated by the Manager, Public Education and Outreach of the OPC Communications Branch, who is already responsible for the OPC's other social media accounts.

### **Overall approach**

This section covers strategic communications approach and tactics. It addresses:

- Approach to sharing and engaging
- Foundational elements to launch the page (OPC Facebook Comment Policy, OPC Facebook Privacy Notice, Posting guidelines / Service standards )



- Compliance with Government of Canada policies and guidelines (Identity, Official Languages, Accessibility, Publishing, Account configuration and compliance)
- Development of the Facebook Page (Development and branding, Account Verification)
- Ongoing management (Posting, Approval process, Daily management of Facebook page)
- Evaluation

## Communicating and Engaging

The OPC plans to use Facebook as a platform for *sharing content* and *engaging with the public*.

With respect to *sharing content*, the OPC will:

- Communicate the OPC brand as a protector and promoter of privacy rights for all Canadians.
- Adopt a tone that is friendly, helpful, and approachable, keeping in mind that its target audience is adults with children and elderly parents; and
- Share existing and new OPC resources developed for individuals; inform the public of relevant news and announcements from our Office; and share relevant Facebook posts from other DPAs and other federal government organizations (e.g. Public Safety's Get Cyber Safe Facebook Page and Innovation, Science and Economic Development's Your Money Matters Facebook page).

With respect to *engaging the public*, in addition to the above, the OPC will:

- Be timely, accurate, clear, objective, responsive, respectful and fair in its communications with the public, as per our obligations under the Government of Canada's Policy on Communications and Federal Identity and the Government of Canada's Values and Ethics Code.
- Ensure our organizational use of Facebook is in compliance with internal and external guidelines, policies and legislation with respect to privacy; and
- Be transparent and open about our expectations and practices regarding users communicating with our Office via Facebook. (See the proposed Facebook Comment Policy below.)

## Foundational elements

In order to launch the Page, the OPC must develop or establish a few key foundational pieces: a Comment Policy, Privacy Notice, Terms of Engagement and the Service Standard. Users can read more about these in our "Third-Party Social Media" section in the following link:

<https://www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/terms-and-conditions-of-use/#privacy>

### *OPC Facebook Comment Policy*

Comments left on posts are made public on the Page automatically and immediately. A notification is also sent to the Administrators.

Administrators will review the comment and, if the comment meets any of the following conditions mentioned in the comment policy below, the comment will be hidden from the post. The Facebook Page will be monitored during business hours (Monday – Friday, 8:30am to 5:00 pm). Our Facebook Page will

indicate that the Page is monitored regularly during these hours. Comments may occasionally be reviewed outside of business hours (evenings, weekends and statutory holidays).

Comments left on our Page that meet any of the following conditions outlined in our Facebook Comment Policy may be edited or removed by the administrators of our Page. These will be reviewed on a case by case basis, consulting with Legal, Policy and others as appropriate. If a comment appears to add to the discussion but includes, for example, personal information, administrators may also choose to send a message to the individual user explaining why their comment has been removed. As a general practice, however, we will not notify users when we remove a comment.

The Comment Policy will be posted directly on our Facebook page. This draft Comment Policy, and the Privacy Notice below, have been approved by the Commissioner when this document was originally approved, August 15, 2016.). The Comment Policy and Privacy Notice were further reviewed and revised by Legal Services, September 8, 2016.).

Here is the proposed text for the Comment Policy:

*All comments posted by Facebook users to the OPC's Facebook page, as well as messages sent to the OPC via Facebook will be reviewed by OPC staff with administrator rights to the page. Although we are not able to reply individually to all posts, comments and messages, they will be handled on a case-by-case basis and responded to when deemed appropriate.*

*The OPC cannot and does not provide advance rulings with respect to privacy issues on Facebook. We encourage you to contact the OPC's Information Centre with any privacy-related questions or concerns.*

*We reserve the right to edit or remove comments that meet any of the following conditions:*

- *are contrary to the principles of the Canadian Charter of Rights and Freedoms;*
- *are racist, hateful, sexist, homophobic, defamatory, insulting, threatening, or otherwise discriminating or hurtful to an individual or group;*
- *put forward serious, unproven or inaccurate accusations against individuals or organizations;*
- *are aggressive, vulgar, indecent, rude, abusive, coarse, violent, obscene or pornographic in tone or content;*
- *are offensive, defamatory, disparaging or include defamatory statements to an individual or an organization;*
- *are not sent by the author and/or posted by anonymous or robot accounts;*
- *are put forward for phishing or spamming purposes;*
- *are written in a language other than English or French;*
- *are solicitations, advertisements, or endorsements of any financial, commercial or non-governmental agency;*
- *contain announcements from labour or political organizations;*
- *contain personal information about you or any other person;*
- *contain any names, products or services, logos, slogans, mascots, artwork, or promotion of any brand, product or service of any company or entity, or any material protected by copyright or trademarks;*
- *are unintelligible or irrelevant to the Page;*

- *encourage or suggest illegal activity;*
- *are repetitive or spamming of threads, and*
- *do not, in the moderators' opinion, add to the normal flow of the discussion.*

#### *OPC Facebook Privacy Notice*

The Privacy Notice will be posted directly on our Facebook page. Here is the proposed wording for our Privacy Notice, reviewed by Legal:

*Facebook is a third-party service provider used by the Office of the Privacy Commissioner of Canada to communicate with the public. Facebook account holders who use the service are bound by Facebook's Terms of Service and Privacy Policy – this includes our Office, and individuals who communicate with our Office via Facebook. We encourage users to read Facebook's Terms of Service and Privacy Policy, as well as the Terms of Service and Privacy Policies for all social networking services they use.*

*Comments left by individuals on the OPC's Facebook Page can be read by anyone. Therefore, we strongly advise users not to post personal information – either their own, or the information of others – on our Facebook Page. As per our Facebook Comment Policy, the OPC reserves the right to remove any comments containing personal information.*

*The amount of information about a user that is available publicly depends on the user's privacy settings. The OPC reminds users to regularly check and adjust individual privacy settings as they may change over time.*

*Our Office may use information you provide on Facebook – including, but not limited to the personal opinions contained in your comments or messages to us – for statistical or analytical purposes.*

*Should you have any questions about your privacy rights as explained in this Privacy Notice, please contact our Chief Privacy Officer, who is also the Director of the Access to Information and Privacy Unit, through our toll-free line at 1-800-282-1376, or by postal mail at:*

*30 Victoria St.  
Gatineau, Quebec  
K1A 1H3*

#### *Posting guidelines / Service standards*

Feedback and interaction is highly encouraged. All wall posts and comments, as well as email sent to the Facebook account will be read, and any emerging themes or helpful suggestions will be passed to the relevant people in the office.

Although we may not be able to reply individually to all private messages sent to our Facebook account, they will be handled on a case-by-case basis and responded to when deemed appropriate. The OPC will answer messages from the public in a timely manner and will be able to review its response time using the reporting tools in Facebook available to the administrators.

Questions requiring a more elaborate response will be referred to the Information Centre. Individuals putting forward privacy complaints or concerns will be referred to the appropriate section of our website.

Reporters engaging us on Facebook will be asked to send questions to our Media Relations team.

## **Compliance with Government of Canada policies and guidelines**

The following describes some of the key policies, guidelines and laws that can apply to government social media accounts and how we will ensure compliance with those that apply to the OPC.

### *Identity*

The OPC is not subject to the standard visual requirements defined in the TBS Policy on Communications and Federal Identity. This means that we can use the OPC coat-of-arms to identify ourselves on Facebook (instead of the flag) or any image that we deem appropriate.

### *Official Languages*

The OPC respects the Official Languages Act and is committed to ensuring that information products are available in both French and English, of equal quality.

OPC Communications will establish separate Facebook pages in English and in French, as per the approach recommended by the Government of Canada in its Policy on Communications and Federal Identity and in-line with our current use of Twitter.

Comments and questions that require a response will be answered in the official language of origin.

Users should be aware that some links direct users to sites of organizations or other entities that are not subject to the Official Languages Act and that these sources are only available in the language in which they are written. For example, we may choose to share a *New York Times* article only on our English page only, or a *La Presse* article only on our French page. We will aim to have the same number of posts shared in both languages whenever possible, however, there may be quiet days where only relevant posts in one language or the other.

### *Accessibility*

The Government of Canada must comply with Web Content Accessibility Guidelines 2.0 (WCAG), which aims to make content accessible to a wider range of people with disabilities, including blindness and low vision, deafness and hearing loss, learning disabilities, cognitive limitations, limited movement, speech disabilities, photosensitivity and combinations of these. Facebook allows for: compatibility with voiceover software for the visually impaired, captions to be added to videos (in .srt files) and full text to be accompanied with Infographics. Our office, in its commitment to achieving a high standard of accessibility, will ensure that our Facebook posts are accessible to visitors with disabilities and respect our Policy on Accommodating Clients with Disabilities.

### *Publishing*

The OPC complies with section 6.3 of the policy on Procedures for Publishing, ensuring that when communications products are posted on third-party platforms, they are also available on Government of Canada websites. For example, our infographics will be posted on Facebook and will be available on our website as well.

### *Account configuration and compliance*

We will comply with the Government of Canada's Technical specifications for social media accounts when creating our Facebook pages, ensuring that we are:

applying correct social media visual and text identifiers (requirement 2.1);	The Coat-of-arms or other relevant pictures will be used to identify the OPC on Facebook. The short usernames @PrivacyCanada and @ViePriveeCanada will be used to identify us quickly.
incorporating a link to the equivalent account in the other official language, if applicable (requirement 2.2);	A link will be featured in the "About" section on our Facebook pages, leading the user to the equivalent account in the other official language.
incorporating a link to the associated government web page (requirement 2.3); and	Our website is listed in the "About" section on our Facebook pages.
incorporating a social media notice (requirement 2.4)	Our social media notice will be posted directly on our Facebook page in a separate tab.

## **Development of the Facebook Page**

### *Development and branding*

As outlined in the critical path below, OPC Communications will establish separate Facebook pages in English and in French.

The Manager, Public Education and Outreach will lead the design of the page.

The branding will be the same for both accounts, with the OPC's coat of arms used as our identifying picture on Facebook.

We will use two short usernames to identify our pages. We recommend @PrivacyCanada and @ViePriveeCanada. These usernames allow users to easily find our page by typing it directly in Facebook's search bar – the shorter, the better for those typing on Facebook mobile.

Two mock pages have been prepared (English and French) and have been listed as unpublished, where only invited users can preview these pages, pre-launch.

### *Account Verification*

Facebook can verify that a page is authentic for a business or organization. A gray checkmark is added beside the name of the page, which confirms for users that the page is truly managed by the identified organization.

This simple step could reassure Canadians that they are in fact dealing with the OPC on Facebook and not a fake group.

Most government departments have received verification from Facebook, such as Parks Canada, Veterans Ombudsman, Finance, Transport, Library and Archives Canada, Canadian Heritage, etc.

Verification also allows us to use the “Facebook Live” option to livestream our events.

### **Launch**

The OPC’s Facebook page is expected to be launched in the fall of 2016. We will inform our provincial, territorial and international colleagues of the page in advance, and will encourage those with existing Facebook pages to help us promote it. We will also reach out to our stakeholders – including other federal government departments, NGOs and other associations – to inform them of our page and encourage them to “like” or share it in order to build followers.

More information can be found in the steps listed in the [Launch Plan](#).

### **Ongoing management**

#### *Posting*

Communications will develop original content for posts from existing communications and outreach Materials, with an emphasis on those relating to the youth outreach strategy.

Posts can also be tied to special months or days such as Financial Literacy Month, Cybersecurity Awareness month and Pink Shirt day (anti-bullying promotion).

We will also share relevant materials from other organizations as appropriate. For example, we may share relevant material posted by other Government of Canada or data protection authorities’ Facebook accounts.

The number of posts will vary depending on how many appropriate and relevant materials for sharing are identified each week. We will aim to share with our followers one post every couple of days (for example, a news article or item created by another organization such as an international DPA or privacy advocacy organization), and to write one original OPC post on a weekly basis.

Prepared posts can be put into the Facebook publishing tool so that they may be scheduled to appear at a specific time, for example, on statutory holidays when the office is closed.

See **Annex A** for examples of posts.

#### *Approval process*

As with content developed for Twitter, all posts will be reviewed and approved by the Manager, Strategic Communications, and, in certain cases, may also involve approval by the DG, Communications and/or the Commissioner.

The Manager, Strategic Communications, will also review any articles and videos of interest from external sources before they are shared on the OPC page.

#### *Daily management of Facebook page*

As with content for our Twitter accounts, planned content for the OPC's Facebook page reside in a Facebook editorial calendar saved in Officium.

Below are the duties involved with managing both pages:

<b>ACTIVITY</b>	<b>FREQUENCY</b>
Answer questions posted on our wall and private messages. Provide generic answer to longer messages which will require a few days for a response	As needed
Create new content to be posted using existing resources from our website and our previous campaigns when possible	Weekly
Collection and reporting of metrics via the Communications Branch Quarterly Report Provide ideas/solutions to keep Facebook pages alive and useful	Quarterly
Change cover image	quarterly

## **Evaluation**

### *Measurement and Evaluation*

As mentioned earlier, Facebook provides some basic analytics (anonymous and aggregated data) to owners of Facebook pages. The OPC will use this data to evaluate and improve its Facebook outreach strategy. This information will be included in the Communications Branch quarterly report, in which trends and statistics are included on web, media relations, social media, events and exhibits, and information requests.

Success in monitoring and responding to engagement (questions, comments, shares, etc.) will be measured through our response time and can also be measured by positive replies and likes on our responses. Sentiment will be tracked by taking a look at the type of likes (normal, Love, haha, Wow, sad and angry) tagged on our posts. As indicated in our Privacy Notice, we will not collect personal

information as part of our measurement and evaluation efforts. The Insights section provides useful data showing the total views for our posts and how well we have reached and engaged our audience:

**Page Summary** Last 7 days +

Export Data

Results from Oct 14, 2016 - Oct 20, 2016

Organic Paid

**Actions on Page**

October 13 - October 19



We don't have data to show you this week.

**Page Views**

October 13 - October 19



We don't have data to show you this week.

**Page Likes**

October 13 - October 19



We don't have data to show you this week.

**Reach**

October 13 - October 19



We don't have data to show you this week.

**Post Engagements**

October 13 - October 19

26

Post Engagements ▲ 100%



**Videos**

October 13 - October 19

9

Total Video Views ▲ 100%



Your 5 Most Recent Posts

Reach: Organic / Paid Post Clicks Reactions, Comments & Shares

Published	Post	Type	Targeting	Reach	Engagement
10/20/2016 12:17 pm	Once you put your personal information out there, you can't take it back. Watch as our video shows that it's aimed	Video	Targeted	0	0 0
10/20/2016 11:43 am	Zoomer Show Lifestyle Expo for the 45+	Image	Targeted	0	0 0
10/20/2016 11:43 am	Here's an interesting article to read: <a href="http://ottawacitizen.com/news/national/defence-watch-the-mystery-of-the-list">http://ottawacitizen.com/news/national/defence-watch-the-mystery-of-the-list</a>	Image	Targeted	0	0 0



**Critical path**

<b>ACTIVITY</b>	<b>TIMING / FREQUENCY</b>
Develop FB strategy outlining objectives, target audiences, information management and privacy practices, and procedures for posting and engaging with the public (e.g. how are posts approved; who has access rights to post/review comments). Strategy will also outline launch strategy.	June 2016
Present FB strategy and invite comment from CPO, PAWG, Legal.	June-July 2016
Send FB strategy to Commissioner for review and approval	August 2016
Work with communications operations (Jana/Monique) to develop graphic elements for pages	August- September
Develop editorial calendar – ideally, first 2 months	August - September
Create pages (E/F); also complete form for verified account: <a href="https://www.facebook.com/help/contact/356341591197702">https://www.facebook.com/help/contact/356341591197702</a>	Jan 2017
Train backup(s) to post	Jan 2016
Create Facebook pages	Late 2016 – Jan 2017
Obtain approval from Communications and the Commissioner	Late 2016
Go live with our Facebook launch	Feb. 22, 2017

## Annex A – Examples of posts

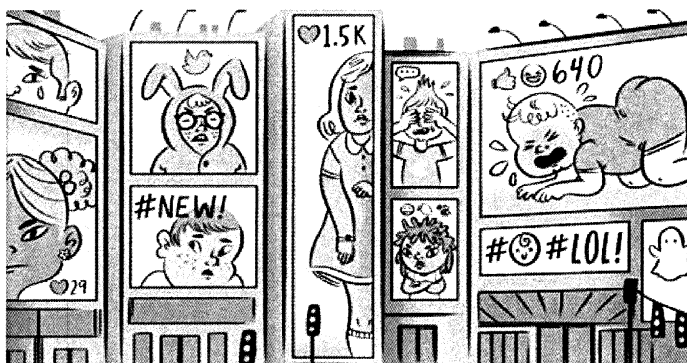
### Sharing articles



Test test test

Published by Pierre-Luc Poirier on 12/02/2014

An interesting read – tell us what you think! <http://www.theatlantic.com/.../2.../10/babies-everywhere/302757/>



#### Giving Kids 'Veto Power' Over a Parent's Facebook Posts

All those Facebook photos are cute—but how are they affecting the kids?

THEATLANTIC.COM | BY ADRIENNE LAFRANCE

### Sharing YouTube videos



Test test test

Published by Pierre-Luc Poirier on 02/02/2014

When the clerk at the store tells you that in order to give you better service they need your phone number, email address, where you were last night, and then they follow you home... That's not okay, right? So why are you giving away all that information to the latest app on your phone? <https://www.youtube.com/watch?v=xYZ8HPRkQg>



#### If your shop assistant was an app (hidden camera)

A large number of apps demand access to your private information such as location, contacts and text messages. How would you react if real people

[youtube.com](https://www.youtube.com/watch?v=xYZ8HPRkQg)



Like Comment Share

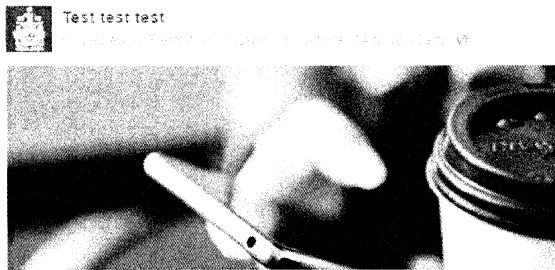


Write a comment

Post your comment

### Facebook Note

Officium 7777-6-146948



## Mobile apps and protecting your personal info

Following the Denmark coffee shop story, here are our tips for protecting your personal information when downloading and using mobile apps: [https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/digital-devices/apps\\_info\\_201405/](https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/digital-devices/apps_info_201405/)

See More

### Video uploaded on our page



Test test test

Published by Pierre-Luc Robitaille on June 11, 2014

Once you put your personal information out there, you can't take it back. Watch as our video shows that it's almost impossible to take back anything that you put online – much like getting the toothpaste back into the tube. Want to know more about protecting your online rep? Check out our website for more tips and tricks - <http://www.youthprivacy.ca>



Boost Unavailable

1,234

Like Comment Share



### OPC post with link



Test test test

Published by Pierre-Luc Robitaille on June 11, 2014

Have you checked your privacy settings lately? Take a look at our ten tips so you can stop the fraudsters helping themselves to your identity [https://www.priv.gc.ca/id/identity-theft/id\\_info\\_201303](https://www.priv.gc.ca/id/identity-theft/id_info_201303)



10 Tips for preventing identity theft - Office of the Privacy Commissioner of Canada

Get some everyday tips for reducing your risk of identity theft.

June 10, 2014

Boost Unavailable

Like Comment Share



Last updated: February 13, 2016

## Facebook Page Launch Plan

The Communications Branch proposes to launch the OPC's new Facebook Page February 22nd.

This document describes key steps required ahead of the launch; sets out the first seven proposed posts for the new Page; and describes how key stakeholders would be advised of the launch and how the OPC would work to build its network of followers.

### Key steps:

#### 1. Completion of foundational elements

Both Facebook pages (English and French) have been created. The Comment Policy and Privacy Notice are available for the user directly on our Facebook page, on the right-hand side menu. The OPC Privacy Policy from our website is also directly highlighted on the Facebook pages.

#### 2. Verification

We will verify both of our pages with Facebook in order to appear as a legitimate organization and to enable the Facebook Live feature. Facebook will verify our pages as soon as they are live. A checkmark is added beside the name of the page, which confirms for users that the page is truly managed by the identified organization.

#### 3. Content development

Our plan is to post one or two items per week.

Here are the seven proposed posts to start:

##### 1. Introduction

Focusing on kids and parents:

2. Pointer to youth resources
3. DYI House rules
4. Twelve quick privacy tips for parents

Posts of general interest:

5. Identity Theft (Income tax season)
6. Do Not Call List
7. Managing App Permissions (Denmark Bakery video)

Please refer to [OPC Facebook Schedule](#) for the full text.

#### 4. Page promotion / building followers

We will work to build visibility for the new page right from the day of the launch. Steps to encourage traffic will include sending email notices to stakeholders and FPT; promoting the page via our other social media channels and GCConnex; and encouraging other organizations to “Like” the page. We will also promote on our website.

##### *Announcement and web promo*

On the day of launch, we would post a brief Announcement on our website.

We will also add a Facebook button on our website in the bottom right corner under the section “Stay Connected,” along with the other social media links.

We would include a slider to promote the Facebook page on our website homepage during the first few weeks after the launch.

##### *Advising staff*

- To ensure OPC staff are aware of the FB page and its purpose, an email will be sent to all staff by the DG Comms, with similar messaging (touching on employee privacy issues) to the message used when the LinkedIn page was announced, given that some staff may choose to “like” or “follow” the OPC FB page.

##### *Advising stakeholders*

- An email from the DG, Communications will be sent through the FPT listserv to let organizations know that the OPC is now on Facebook.
- An email will be sent to privacy advocates (Media Smarts, Digital Tattoo) and our broader stakeholder list, and any other relevant listservs, from the DG, Communications to let them know that the OPC is now on Facebook (as we did when we launched the new website).

##### *Use of other social media channels*

Our Facebook page will be promoted on Twitter, on LinkedIn, on GCConnex, on Facebook by liking pages from other organizations and by email internally and externally.

Here is a brief explanation for each medium to be used:

##### *Twitter, LinkedIn*

We can use these two messages on Twitter and LinkedIn with the OPC’s accounts to reach our followers:

- We are now on Facebook! Come check out our page at <https://www.facebook.com/PrivCanada/>

- Nous sommes désormais sur Facebook! Venez voir notre page au <https://www.facebook.com/ViePriveeCanada>
- Come see us on Facebook, we have info for parents and youth on privacy rights and how to better protect personal information <https://www.facebook.com/PrivCanada/>
- Venez nous voir sur Facebook pour des infos aux parents et jeunes sur droits à la vie privée et protection des renseignements personnels <https://www.facebook.com/ViePriveeCanada>

### *GCconnex*

GCconnex is an effective way to communicate to Government of Canada employees that we are on Facebook. The OPC does not currently have a group page on GCconnex, but communications officers can use their own accounts to send out two messages with this wording on The Wire, GCconnex's own microblog, which behaves much like Twitter.

We will display these messages on GCConnex's Wire:

- We are now on Facebook! Come check out our page at <https://www.facebook.com/PrivCanada/>
- Nous sommes désormais sur Facebook! Venez voir notre page au <https://www.facebook.com/ViePriveeCanada>

### *Liking other pages*

In order to build followers, the OPC will "Like" pages from other organizations, and send a message to these organizations to be liked back: "Hello, we're now on Facebook! We've liked your page and hope you'll consider liking ours. Thanks!"

We will do the same with our French page, using this message: "Bonjour, nous sommes désormais sur Facebook! Nous avons choisi d'aimer votre page et nous espérons que vous choisirez d'aimer la nôtre"

The following is a list of organizations we will Like, to start:

### *Government Departments – Federal and Provincial*

- Senate
- Information Commissioner
- Financial Consumer Agency of Canada (@FCACan and @ACFCan)
- Veterans Ombudsman (@VeteransOmbudsman and @OmbudsmanVeterans)
- Senate (@SenCanada )
- Information Commissioner (@OICCANADA)
- Official Languages Commissioner (@officiallanguages and @languesofficielles)
- Justice (@JusticeCanadaEN and @JusticeCanadaFr)
- Parks Canada (@ParksCanada and @ParcsCanada)
- Canadian Heritage (@CdnHeritage and @Patrimoinecdn)
- National Capital Commission (@NationalCapitalCommission and @CommissionDeLaCapitaleNationale)

- Information and Privacy Commissioner of Ontario (@IPCOntario)
- Healthy Canadians (@HealthyCdns and @CanenSante)
- Get Cyber Safe (@GetCyberSafe and @Pensezcybersecurite)
- Your Money Matters (@YourMoneyMatters and @QuestionsdargentCanada)

*External Organizations*

- Office of the Australian Information Commissioner (@OAICgov)
- Federal Trade Commission (@federaltradecommission)
- Commission Nationale de l'Informatique et des Libertés (@CNIL)
- Information Commissioner's Office (@ICONews)
- Canadian Centre for Child Protection
- MediaSmarts (@MediaSmarts and @HabiloMedias)
- Digital Tattoo (@digitaltattoo)
- Éducaloi (@educaloi)

**Critical path before and during launch day**

<b>ACTIVITY</b>	<b>DATE / FREQUENCY</b>	<b>RESPONSIBILITY</b>
Demo for Commissioner, proceed with steps for approval by Commissioner	Week of February 13	Valerie/AMH/ P-L/AMC
For Web: Ask to prepare the mention of Facebook on our webpage <u>Terms and conditions of use</u> (add to the list of social media platforms in Third-Party Social Media) on launch day  Ask to add the Facebook button in "Stay Connected" on our website on launch day  Prepare home page slider  Prepare Announcement	Week of February 13	Pierre-Luc to liaise with Heather and Monique
Remind Facebook to verify pages on launch date	February 21	P-L
Circulate an email internally to let employees know about the launch	February 21	AMH
<b>LAUNCH DAY</b>	February 22	



<ul style="list-style-type: none"><li>• Put first post on our wall – Introductory post</li><li>• Emails from Anne-Marie Hayden: stakeholders, FPT through ListServ</li><li>• Post Announcement about Facebook launch on OPC website. Alert staff of announcement via email.</li><li>• Promote our Facebook Launch on Twitter and LinkedIn</li><li>• Like pages from other organizations and ask to be Liked back</li><li>• For web: display item on Terms and conditions of use, add Facebook button.</li><li>• Post to GConnex</li><li>• Facebook verifies our pages, adds checkmark</li></ul>		P-L  AMH  MF  AMC  P-L  MF  P-L  P-L
---	--	--

NOTE TO COMMISSIONER

From Valerie Lawton c.c. Anne-Marie Hayden  
Date February 13, 2017  
Subject **OPC Facebook page**

---

Commissioner,

Please find enclosed reference materials related to the upcoming launch of the OPC's Facebook page. These will be discussed at your Communications bilat this Wednesday.

The Facebook Page itself will be shown on screen.

**Facebook Page Launch – steps**

[https://officium/\\_layouts/15/OPC.Officium/Utilities/OfficiumIDLookup.aspx?id=7777-6-169316](https://officium/_layouts/15/OPC.Officium/Utilities/OfficiumIDLookup.aspx?id=7777-6-169316)

*This document discusses final steps prior to launching, including plans for beginning to promote the page and build followers.*

**Proposed first posts – OPC Facebook Schedule:**

[https://officium/\\_layouts/15/OPC.Officium/Utilities/OfficiumIDLookup.aspx?id=7777-6-183830](https://officium/_layouts/15/OPC.Officium/Utilities/OfficiumIDLookup.aspx?id=7777-6-183830)

*This document provides examples of initial posts for the OPC Facebook page. These posts point to OPC resources as well as helpful and/or interesting information offered by other organizations.*

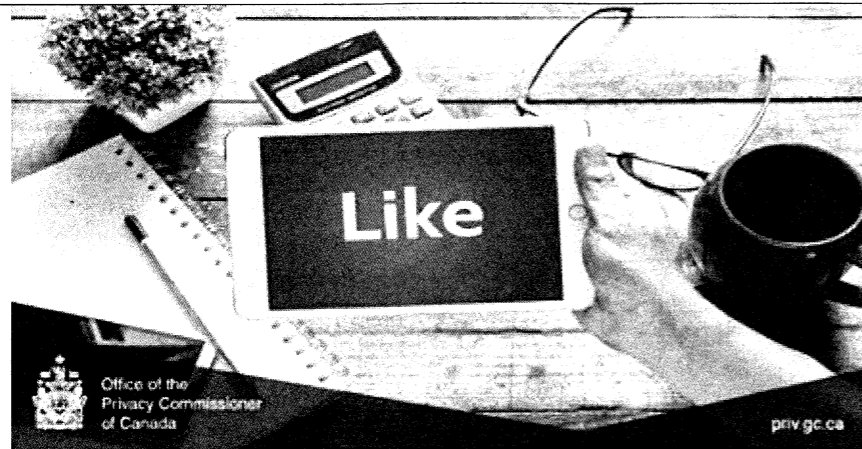
**Facebook Strategy:**

<https://officium/OPS%20%20003300%20%20Develop%20and%20Deliver%20Strategic%20Communi/Fac ebook%20Page%20strategy.docx>

*For reference, the Facebook strategy you've previously approved.*

## OPC Facebook – Examples of initial posts

TOPIC	ENGLISH	FRENCH
<b>Introduction</b>	<p>Surveys tell us that Canadians are increasingly concerned about privacy. In this digital age, more and more personal information is collected, analyzed and used. It's no wonder that many people feel that their ability to protect their personal information is diminishing.</p> <p>The Office of the Privacy Commissioner of Canada has launched this Facebook page to help share information about privacy, your rights and how to protect your personal information.</p> <p>We'll use this space to offer information and tips that we hope will be useful to anyone.</p> <p>We know many parents are on Facebook. With that in mind, we'll especially provide information to help mums and dads talk to their kids about how to avoid privacy pitfalls in the digital world.</p> <p>Join our page to keep up with all our posts!</p> <p>To read the findings from our surveys:  <a href="https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2015/por_2014_12/?WT.mc_id=fb-en-1">https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2015/por_2014_12/?WT.mc_id=fb-en-1</a></p>	<p>Des sondages menés pour le compte du Commissariat ont révélé que les Canadiens se préoccupent de plus en plus de leur vie privée. Dans cette ère numérique, de plus en plus de renseignements personnels sont recueillis, analysés et utilisés. Il n'est pas surprenant que bien des gens ont l'impression qu'ils ne peuvent plus aussi bien protéger leurs renseignements personnels.</p> <p>Le Commissariat à la protection de la vie privée du Canada a lancé sa page Facebook afin de partager avec vous plus d'information sur la vie privée, vos droits et comment protéger vos renseignements personnels.</p> <p>Nous utiliserons cet espace pour offrir de l'information et des conseils utiles à tous.</p> <p>Nous savons que bon nombre de parents sont inscrits à Facebook. Dans cette optique, nous fournirons plus particulièrement de l'information pour aider les parents à éviter les pièges liés à la protection de la vie privée que posent le monde numérique.</p> <p>Suivez-nous sur notre page Facebook et rester à l'affût de nos billets!</p> <p>Pour consulter les résultats de nos sondages: <a href="https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2015/por_2014_12/?WT.mc_id=fb-fr-1">https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2015/por_2014_12/?WT.mc_id=fb-fr-1</a></p>



**DYI House Rules**

Setting house rules that protect your child's privacy in our ever-changing digital world isn't always easy. We're here to help with an easy-to-use DIY house rules tool!

It's easy...Just check off all of the house rules that apply to your family and print off the dos and don'ts for your children:

[https://www.priv.gc.ca/biens-assets/youth-plan/index1\\_e/?WT.mc\\_id=fb-en-2](https://www.priv.gc.ca/biens-assets/youth-plan/index1_e/?WT.mc_id=fb-en-2)

Create your own  
House Rules



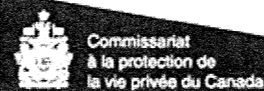
priv.gc.ca

Élaborer des règles à la maison qui protègent les renseignements personnels de vos enfants n'est pas toujours facile dans un monde numérique en constante évolution. Nous sommes là pour vous aider et grâce à cet outil pratique, vous pourrez élaborer des règles pour votre foyer!

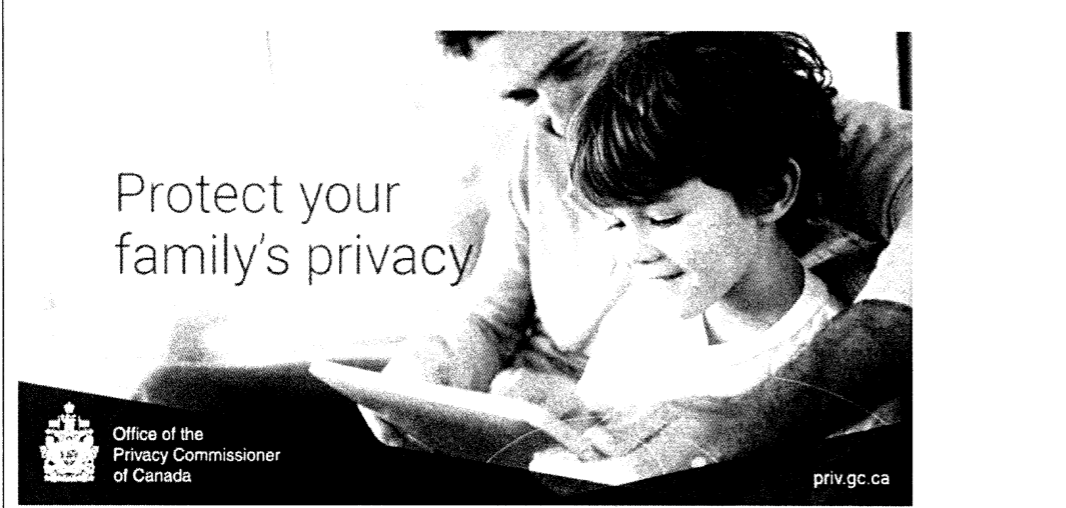

C'est simple...Vous n'avez qu'à choisir les règles à la maison qui s'appliquent à votre famille puis d'imprimer les choses à faire et à ne pas faire pour vos enfants :

[https://www.priv.gc.ca/biens-assets/youth-plan/index1\\_f/?WT.mc\\_id=fb-fr-2](https://www.priv.gc.ca/biens-assets/youth-plan/index1_f/?WT.mc_id=fb-fr-2)

Créez vos propres  
règles à la maison



priv.gc.ca

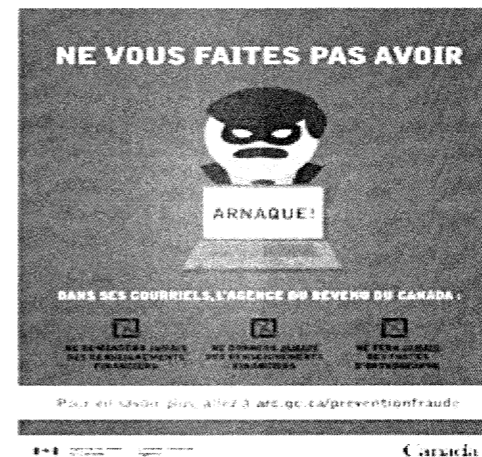
<p><b>General</b></p>	<p>Your kids are avid Internet users and are growing up in a world powered by technology. But the line between private and public information online is getting blurred. We're here to help!</p> <p>We have a ton of resources to help guide you and your kids in the right direction in this ever changing digital world!</p> <p>To learn more about privacy and your kids: <a href="https://www.priv.gc.ca/en/privacy-topics/privacy-and-kids/?WT.mc_id=fb-en-3">https://www.priv.gc.ca/en/privacy-topics/privacy-and-kids/?WT.mc_id=fb-en-3</a></p> 	<p>Vos enfants sont des internautes aguerris. Ils grandissent dans un monde propulsé par la technologie ce qui a brouillé la frontière entre l'information privée et publique en ligne. Nous sommes là pour vous aider à vous y retrouver!</p> <p>Nous avons une panoplie de ressources pour vous aider à guider vos enfants dans la bonne direction dans ce monde numérique en constante évolution : <a href="https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-de-la-vie-privee-et-enfants/?WT.mc_id=fb-fr-3">https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-de-la-vie-privee-et-enfants/?WT.mc_id=fb-fr-3</a></p> 
<p><b>Identity Theft (Income tax season)</b></p>	<p>It's income tax season and taxpayers should be vigilant when contacted by somebody who claims to be from the Canada Revenue Agency (CRA) or another government body. Whether contacted by phone, mail, text message or email, there's a good chance you're being targeted by a scam. Do not click on any links or give out your social insurance number, credit card number, bank account number or passport number, even if the individual insists this personal information is needed if you are to receive your refund or benefit payment. The CRA and other government departments do not send emails with</p>	<p>C'est la saison des impôts et les contribuables devraient faire preuve de vigilance lorsqu'ils reçoivent un appel, courrier, message texte ou courriel d'un individu soi-disant de l'Agence du revenu du Canada (ARC) ou d'un autre organisme gouvernemental. Il y a de fortes chances que vous soyez l'objet d'une arnaque. Ne cliquez sur aucun lien et ne communiquez pas votre numéro d'assurance sociale, numéro de carte de crédit, numéro de compte bancaire ou numéro de passeport même si l'individu insiste sur le fait que ces renseignements personnels sont nécessaires pour que vous puissiez recevoir</p>



links or ask you to divulge personal or financial information in this manner.  
More information on how to prevent this type of fraud can be found on CRA's website: <http://www.cra-arc.gc.ca/scrty/frdprvntn/menu-eng.html>



un remboursement ou un versement de prestation. L'ARC et d'autres ministères n'envoient pas de courriels contenant des liens ou ne vous demandent pas de divulguer des renseignements personnels ou financiers de cette façon.

De plus amples renseignements pour vous prémunir contre ce type de vol d'identité sont disponibles sur le site web de l'ARC: <http://www.cra-arc.gc.ca/scrty/frdprvntn/menu-fra.html>



<p><b>Tips for parents</b></p>	<p>Hi parents!</p> <p>Take a few minutes to check out our 12 quick privacy tips to help your kids understand the impact that some online activities may have on their privacy: <a href="https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/fs-fi/tips/?WT.mc_id=fb-en-4">https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/fs-fi/tips/?WT.mc_id=fb-en-4</a></p>  <p>The advertisement features a black and white photograph of a man and a young child sitting together, looking at a tablet. The text '12 Privacy Tips for Parents' is prominently displayed in the upper left. At the bottom left is the logo of the Office of the Privacy Commissioner of Canada, and at the bottom right is the website 'priv.gc.ca'.</p>	<p>Allô les parents!</p> <p>Prenez quelques minutes pour consulter nos 12 conseils pour vous aider à expliquer à vos enfants les répercussions que certaines activités en ligne peuvent avoir sur la protection de leur vie privée : <a href="https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/campagnes-et-activites-de-sensibilisation/sensibilisation-des-enfants-a-la-vie-privee/fs-fi/tips/?WT.mc_id=fb-fr-4">https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/campagnes-et-activites-de-sensibilisation/sensibilisation-des-enfants-a-la-vie-privee/fs-fi/tips/?WT.mc_id=fb-fr-4</a></p>  <p>The advertisement features a black and white photograph of a man and a young child sitting together, looking at a tablet. The text '12 conseils sur la vie privée pour les parents' is prominently displayed in the upper left. At the bottom left is the logo of the Commissariat à la protection de la vie privée du Canada, and at the bottom right is the website 'priv.gc.ca'.</p>
<p><b>Do Not Call List</b></p>	<p>Do you receive unwanted calls from telemarketers? You may want to consider registering your number on the Do Not Call list (DNCL): <a href="https://www.lnnte-dncl.gc.ca/insnum-regnum-eng">https://www.lnnte-dncl.gc.ca/insnum-regnum-eng</a></p>	<p>Avez-vous reçu des appels non sollicités de firmes de télémarketing? Vous pouvez mettre fin à ce genre d'appel en inscrivant votre numéro de téléphone à la liste nationale de numéros de télécommunication exclus: <a href="https://www.lnnte-dncl.gc.ca/insnum-regnum-fra">https://www.lnnte-dncl.gc.ca/insnum-regnum-fra</a></p>



**Denmark Bakery**

If store clerks insisted on knowing your phone number, accessing your telephone contacts and where you were last night, you'd undoubtedly feel more than a little uncomfortable. But have you considered how much personal information you're providing to the latest app on your smart phone?

A Denmark bakery gave customers a taste of what app permissions might look like in real world. Check out their video below, and read our tips for protecting your personal information when downloading and using mobile apps: [https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/digital-devices/apps\\_info\\_201405/?WT.mc\\_id=fb-en-5](https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/digital-devices/apps_info_201405/?WT.mc_id=fb-en-5)

<https://www.youtube.com/watch?v=xYZtHIPktQg>

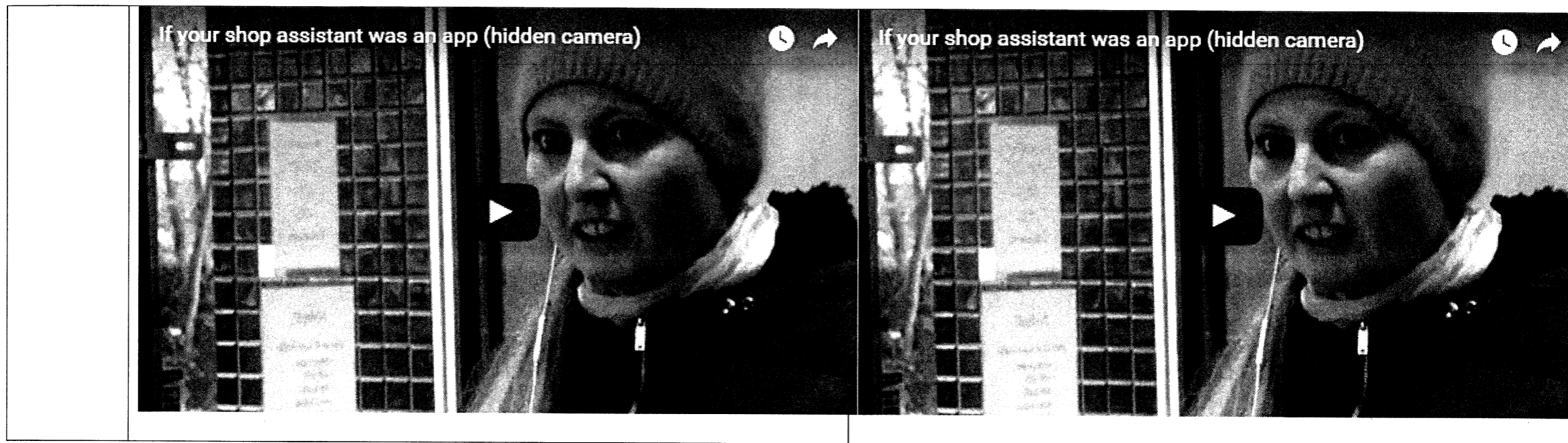
Si les commis d'un magasin insistaient pour obtenir votre numéro de téléphone, pour avoir accès aux numéros de vos contacts personnels, ou encore exigeaient de savoir où vous étiez hier soir, vous vous sentiriez probablement inconfortable. Mais est-ce vous vous êtes déjà arrêté pour réfléchir à la quantité de renseignements personnels que vous fournissez par l'entremise de la dernière application installée sur votre téléphone intelligent?

Une boulangerie au Danemark a donné un avant-goût à ses clients de ce qu'ont l'air dans la vie de tous les jours les permissions exigées par les applications (en anglais seulement). Prenez quelques minutes pour visionner leur vidéo affichée ci-dessous, et pour lire nos conseils pour protéger vos renseignements personnels lors du téléchargement et de l'utilisation d'applications mobiles: [https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie-et-vie-privee/appareils-numeriques/apps\\_info\\_201405/?WT.mc\\_id=fb-fr-5](https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie-et-vie-privee/appareils-numeriques/apps_info_201405/?WT.mc_id=fb-fr-5)

*Veillez noter que cette vidéo n'est disponible qu'en anglais seulement.*

<https://www.youtube.com/watch?v=xYZtHIPktQg>





Commissariat  
à la protection de  
la vie privée du  
CanadaOffice of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
	2 + attachments

**NOTE D'INFORMATION****BRIEFING NOTE**

### National Security Consultations Timelines and Outline

**OBJET / PURPOSE:** To inform you of the way forward for the Public Safety consultations on National Security.

**CONTEXTE / BACKGROUND:**

Further to a briefing note prepared for you on this matter, and subsequent meetings, you will find attached an outline document which will form the basis of the Office's submission to the above-referenced consultations. The outline follows the structure of the consultation backgrounder "Our Security, Our Rights: National Security Green Paper, 2016"<sup>1</sup> and includes placeholders for what will eventually become the submission text. It includes endnote references which point to pre-existing material which can be drawn upon.

You will receive portions of proposed text for your review prior to each meeting, the dates of which are already in your calendar.

For the purposes of translation, and in order to ensure we meet Public Safety's submission deadline of December 1, we propose limiting ourselves to a maximum of 15 pages.

**CONSULTATIONS:** Legal Services (Julia Barss, Michael Sims, Sarah Speevak)

**RELATED DOCUMENTS / DOCUMENTS CONNEXES:**


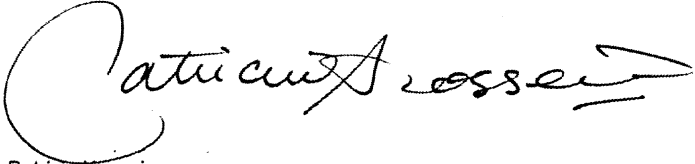
- Submission on National Security Consultations (Public Safety Canada) 7777-6-164260
- Public Safety National Security consultation backgrounder - Our Security, Our Rights 7777-6-164257
- Briefing Note - participation in Public Safety's consultations on national security - September 2016 7777-6-162822

**DISTRIBUTION:** Commissioner, LSPRTA


**APPROBATION / APPROVAL:**

Rédigé par / Prepared by	Date	Revisions
Leslie Fournier-Dupelle	September 22, 2016	

<sup>1</sup> Available online at <http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-scart-grn-ppr-2016-bckgrndr/index-en.aspx> and in Officium at 7777-6-164257

Approuvé par / Approved by	Date
	23/9/16
Barbara Bucknell Directrice, Politiques et recherche / Director, Policy and Research	
Approuvé par – Approuvé par	Date
	23/9/16
Patricia Kosseim Avocate générale principale et Directrice générale / Senior General Counsel	
Approuvé par / Approved by	Date
<input type="checkbox"/> Je suis satisfait des mesures proposées. / I agree with the proposed recommendation(s). <input checked="" type="checkbox"/> Je ne suis pas satisfait de ces recommandations pour les raisons suivantes. / I do not agree with the proposed recommendation(s) for the following reason(s): Commentaires ou des instructions supplémentaires / Additional Comments or Instructions: I would not assume that the structure & content within the 8 chapters or issues will be as proposed: that should be discussed & agreed upon at the meetings I have scheduled. Glad to discuss what that means for your prep work & whether the meetings are too late to "land" by Dec. 1.	
Daniel Therrien Le commissaire à la protection de la vie privée / Privacy Commissioner	

In addition, I may want to "land" before Dec. 1 so as to be available for the media upon publication and, ideally, also attend APPA.

  
23/9/16

December 5, 2016

National Security Policy Directorate  
Public Safety Canada  
269 Laurier Avenue West  
Ottawa, Ontario K1A 0P8  
[ps.nsconsultation-consultationsn.sp@canada.ca](mailto:ps.nsconsultation-consultationsn.sp@canada.ca)

**Subject: Consultation on Canada's National Security Framework**

Dear Sir/Madam:

I, along with my provincial and territorial counterparts, would like to take this opportunity to respond to the Call for Submissions issued on September 8, 2016 in support of the consultation on key elements of Canada's national security laws and policies to ensure they reflect the rights, values and freedoms of Canadians. Our Offices oversee compliance with federal, provincial and territorial privacy legislation and, as such, are responsible for protecting and promoting privacy rights of individuals.

***Introduction***

We note that the stated purpose of the National Security Green Paper is to “prompt discussion and debate about Canada’s national security framework,” which is broader than the reforms brought about by Bill C-51, the *Anti-Terrorism Act*, 2015. We fully support the need to review the entire framework. Bill C-51 is only part, even a small part, of the national security laws in force in Canada and it would be a mistake to only review the most recent addition to an important edifice. But to do that in a comprehensive way, the focus cannot be only on addressing challenges faced by national security and law enforcement agencies.

National security agencies have an important and difficult mandate in protecting all Canadians from terrorist threats, and we believe they generally strive to do their work in a way that respects human rights. But history has shown us that serious human rights abuses can occur, not only abroad but in Canada, in the name of national security.

In order to ensure our laws adapt to current realities, it is important to consider all that we have learned before and after 2001, including the revelations of Edward Snowden regarding mass surveillance, other known risks regarding the protection of privacy and human rights such as those identified during commissions of inquiry, as well as recent terrorist threats and incidents.

.../2

Key lessons from this history are that the legal framework should include clearer safeguards to protect rights and prevent abuse, that national security agencies must be subject to effective and comprehensive review, and that new state powers must be justified on the basis of evidence.

### *Accountability*

We are in full agreement with the Green Paper's statement that "effective accountability mechanisms are key to maintaining the public's trust in [intelligence and national security] agencies."<sup>1</sup> However, the proposed creation of a new National Security and Intelligence Committee of Parliamentarians as envisaged by C-22, although a welcome step in the right direction, is insufficient. We note that other countries have implemented an oversight model which includes review by a Committee of Parliamentarians, while maintaining review by experts. While the former provides democratic accountability, the latter ensures that in-depth knowledge of the operations of national security agencies and of relevant areas of the law are applied so that rights are effectively protected. There are, however, still gaps in coverage in Canada by expert review bodies. Of the 17 agencies authorized to receive information under the *Security of Canada Information Sharing Act* (SCISA), only three are currently subject to expert review. As well, there are other government institutions which have a role in national security, including the Privy Council Office.

The Green Paper notes that in some countries, expert review takes the form of a consolidated model, meaning one review body is responsible for all relevant government institutions – a so-called "Super-SIRC" – whereas in others, different bodies are limited to reviewing one institution or one aspect of national security activities. We have no strong preference between the two models, so long as all government institutions involved in national security are covered. Furthermore, if there is more than one review body, all bodies must be able to collaborate in their review activities, and no longer operate in silos.

Among the models in place around the world is the US model where one body, the Privacy and Civil Liberties Oversight Board, is responsible for reviewing the activities of a number of national security agencies for compliance with both privacy and other human rights. Importing that concept in Canada might mean creating a "fully consolidated model", where a single body would be responsible for reviewing all government institutions and all areas of the law.

While such a model would have some merit, we believe it is preferable to have the activities of national security agencies reviewed both by the Office of the Privacy Commissioner and either a single or multiple dedicated national security review bodies. This creates some

.../3

---

<sup>1</sup> Our Security, Our Rights: National Security Green Paper, Background Document 2016, p.9

- 3 -

overlap, but it ensures that both national security and privacy can be examined by experts with deep and broad knowledge of both privacy and national security law. Among other factors, there is value in having the privacy impact of the work of national security agencies reviewed by an institution that also reviews the work of other government departments, so that best practices and developments in privacy law can apply across government.

As mentioned, review bodies must be able to share information, including classified and personal information, so that their respective reviews can be performed in a collaborative and effective manner rather than in silos as is currently the case. The detriments to siloed review include duplication of effort with resulting effects on resources, but above all less informed and therefore less effective review by all relevant bodies. Given the OPC's extensive and ongoing work in this area, it should be included among the review bodies granted the authority to share and receive information.

Minister Goodale acknowledged that the OPC is a “key part of the parliamentary oversight and accountability apparatus.”<sup>2</sup> This reflects the fact that information, including personal information, is a necessary ingredient in the work of national security agencies, many of which call information their “lifeblood.” Currently, the confidentiality provisions of the *Privacy Act* prevent the OPC from sharing information with other review bodies, such as the Security Intelligence Review Committee (SIRC), the Office of the Communications Security Establishment Commissioner (OCSEC) or the Civilian Review and Complaints Commission for the RCMP concerning ongoing investigations into national security practices. A system which proposes removal of silos between government departments for information sharing purposes in the name of national security must provide for the same removal of silos for the review bodies which ensure their activities comply with the law.

In order to be fully effective, review bodies must also be properly resourced. Greatly enhanced national security activities and initiatives in recent years have resulted in much heightened public concerns about privacy, including mass surveillance, but without any consequential increase in funding for the oversight bodies. For the OPC's part, it has been forced to risk manage its limited resources, moving efforts from other mandated activities. This is less than ideal. It is also insufficient to produce effective review and privacy oversight, which are essential to maintain trust in national security activities.

.../4

---

<sup>2</sup> Hon. Ralph Goodale (Minister of Public Safety and Emergency Preparedness), appearance before the Standing Committee on Public Safety and National Security, October 6, 2016 (at 1535).

- 4 -

The OPC's research on oversight of security and intelligence agencies has led it to determine that, beyond resourcing, effective review requires meaningful independence from the executive, non-partisanship and institutional expertise, with knowledge of both domestic and international standards and law.<sup>3</sup>

### ***Prevention***

The Green Paper indicates the path to terrorism begins with “radicalization to violence,” and describes a number of preventative activities which can be undertaken to counteract radicalization.<sup>4</sup> While there is unquestioned value in community engagement, conduct of research and promotion of alternative narratives, we would be concerned if prevention activities, which include detection efforts, involved widespread internet monitoring. By creating a situation where people feel inhibited or censor themselves for fear that their views may be misinterpreted, they may turn away from using this important tool for personal development and for exploring ideas. There is some evidence this may already be happening: a recent study by the US Pew Research Center revealed that nearly nine-in-ten respondents had heard of government surveillance programs to monitor phone use and internet use and of those, a quarter had changed their online habits.<sup>5</sup>

There is a privacy interest in much that we do online, and the expectation of privacy will vary according to the context: a private “direct message” between users on a social media network will likely engage a greater expectation of privacy than, say, a public tweet. Furthermore, the perception exists that person-to-person e-mails are private communications, however vulnerable they are to interception. The intrusiveness of proposed “prevention activities” must take this fact into account. Overall, while we appreciate that countering radicalization is a legitimate goal, we advocate a balanced approach which limits the potential chilling effect and focuses prevention activities or detection efforts on what reliable intelligence reveals are credible threats.

.../5

---

<sup>3</sup> This research included reviews of previous Commissions of Inquiry, reports and research from stakeholders, other review bodies and academic literature.

<sup>4</sup> Our Security, Our Rights: National Security Green Paper, Background Document, 2016, p. 15

<sup>5</sup> Americans' Privacy Strategies Post-Snowden, March 2015 (<http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/>)

## ***Domestic National Security Information Sharing***

The concerns we have in this area, as articulated in the OPC's previous submissions to the Standing Senate Committee on National Security and Defence<sup>6</sup> and Standing Committee on Public Safety and National Security of the House of Commons,<sup>7</sup> remain. We recognize that protecting the security of Canadians is important, and that in order to do so, greater information sharing may sometimes lead to the identification and suppression of security threats. However, the scale of information sharing put in place by SCISA is unprecedented, the scope of the new powers conferred is excessive, particularly as these powers affect ordinary Canadians, and the safeguards protecting against unreasonable loss of privacy are seriously deficient.

### **(I) NEED FOR EVIDENTIARY BASIS**

Given that increased information sharing affects privacy and other rights, the justification for SCISA should be made clear. We have yet to hear a compelling explanation, with practical examples, of how the previous law created impediments to information sharing operationally required for national security purposes. When Bill C-51 was introduced in Parliament, the government maintained that SCISA was necessary because some federal agencies lacked clear legal authority to share information related to national security. The Green Paper speaks to complexity around sharing which can “prevent information from getting to the right institution in time.”<sup>8</sup> These references to the “complexity” of the old law do not explain its shortcomings or how it frustrated the government's national security operations. Situations where legal authority was lacking should be identified, but so far they have not been. A clearer articulation of the problems with the previous law would help define a proportionate solution.

### **(II) RELEVANCE AS THE LEGAL STANDARD**

We remain concerned that SCISA authorizes information to be shared where it is merely of “relevance” to national security goals. Setting such a low standard is a key reason why the risks to law abiding citizens are excessive. Revelations by Edward Snowden have shown how pervasive government surveillance programs can be, including some in place in Canada, and how they can affect all Canadians, not only those suspected of being a terrorist threat. If “strictly

.../6

---

<sup>6</sup> OPC's Submission to the Standing Senate Committee on National Security and Defence on Bill C-51, *the Anti-Terrorism Act, 2015* ([https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl\\_sub\\_150416/](https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl_sub_150416/))

<sup>7</sup> OPC's Submission to the Standing Committee on Public Safety and National Security of the House of Commons on Bill C-51, *the Anti-Terrorism Act, 2015* ([https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl\\_sub\\_150305/](https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl_sub_150305/))

<sup>8</sup> Our Security, Our Rights: National Security Green Paper, Background Document, 2016, p. 26.



necessary”<sup>9</sup> is adequate for CSIS to collect, analyze and retain information, as has been the case since its inception, it is unclear to us why this cannot be adopted as a standard for information sharing for *all* departments and agencies with a stake in national security. Necessity and proportionality are the applicable legal standards in Europe. European law permits member states to interfere with a citizen’s protected privacy rights only to the extent that the interference is necessary and proportionate in a democratic society.

As an alternative to adopting a “necessity and proportionality” standard for information-sharing across the board, consideration could be given to adopting dual thresholds, one for the disclosing institutions, and another for the 17 recipient institutions. An important point raised by departmental officials during the current review of SCISA by the Standing Committee on Access to Information, Privacy and Ethics is that because front line staff in non-listed departments do not necessarily have the requisite expertise or experience to make real-time and nuanced decisions as to what is necessary and proportional for purposes of carrying out a national security mandate, the onus of the higher threshold would be shifted to the 17 recipient departments that do have the capacity to make such decisions in an informed manner. The Committee discussed the issue of a “dual threshold” and this would appear a reasonable solution under the following condition. In order to close the triage gap between these two different thresholds, the 17 recipient departments should be responsible for selectively receiving and retaining only information that meets the higher threshold of necessity and proportionality (subject to any further limits imposed by their enabling laws), and under a positive legal obligation to return or destroy information that does not.

It should be noted that any changes made or contemplated which involve Canada’s national security activities could affect the European Union’s assessment of Canada’s status as an adequate jurisdiction towards which the personal data of the European citizens can be transferred. According to the European Court of Justice’s decision in *Schrems*<sup>10</sup>, necessity and proportionality are important considerations to maintain that status. This decision could have consequential implications for Canada’s trade relationship with the EU.

### **(III) DATA RETENTION**

An issue of equal importance which the OPC has flagged in previous submissions is the setting of clear limits around how long information received or shared is to be retained. If the government maintains that the sharing of information about ordinary citizens (such as travelers or taxpayers) to one or more of the 17 recipient institutions under SCISA is necessary to undertake

.../7

---

<sup>9</sup> S. 12, *Canadian Security Intelligence Service Act* (R.S.C., 1985, c. C-23)

<sup>10</sup> Court of Justice of the European Union, *Maximilian Schrems v Data Protection Commissioner* (6 October 2015) (<http://eur-lex.europa.eu/legal-content/EN/SUM/?uri=CELEX:62014CJ0362>)

analyses meant to detect new threats, national security agencies should be required to dispose of that information immediately after these analyses are completed and the vast majority of individuals have been cleared of any suspected terrorist activities. This would be in keeping with the recent judgment of the Federal Court which held that retention of "associated data" for people who are not a threat to national security was illegal.<sup>11</sup>

#### **(IV) INFORMATION SHARING AGREEMENTS**

We maintain the need for an explicit requirement for written information agreements, as the OPC recommended in the context of Bill C-51.<sup>12</sup> These agreements, far from being cumbersome or unworkable, could be drafted at a level of specificity beyond what the statute provides but still remain general enough to be operationally flexible. They need not be at the individual activity level but rather designed to govern information sharing at the level of programs specific to departments, and could provide more specificity beyond the core standards. Elements addressed in these Agreements should include, as a legal requirement, the specific elements of personal information being shared; the specific purposes for the sharing; limitations on secondary use and onward transfer; and other measures to be prescribed by regulations, such as specific safeguards, retention periods and accountability measures. The OPC has, in the context of *Privacy Act* reform, recommended that it should be notified of all new or amended agreements to share personal information. The OPC should also be given explicit authority to review and comment, and the right to review existing agreements on request by OPC to assess compliance. Finally, departments should be required to publish the existence and nature of information-sharing agreements between departments or with other governments.<sup>13</sup>

#### **(V) PRIVACY IMPACT ASSESSMENTS**

An additional tool to determine whether government initiatives involving the use of personal information raise privacy risks is the Privacy Impact Assessment (PIA), which describes and quantifies these risks, and proposes solutions to eliminate or mitigate them to an acceptable level. At the federal level, the obligation to conduct PIAs is currently at the policy level, and is

.../8

---

<sup>11</sup> 2016 FC 1105. See also the discussion at pages 10-11 of the European Court of Justice decision invalidating the 2006 EU Data Retention Directive.

<sup>12</sup> OPC's Submission to the Standing Senate Committee on National Security and Defence on Bill C-51, *the Anti-Terrorism Act, 2015* ([https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl\\_sub\\_150416/](https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl_sub_150416/))

<sup>13</sup> *Privacy Act* Reform in an Era of Change and Transparency: recommendation 1 ([https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl\\_sub\\_160322/#toc1\\_1a](https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_160322/#toc1_1a))

triggered by a new or substantially modified program or activity.<sup>14</sup> Despite this policy obligation, the OPC was concerned to see how few PIAs were undertaken in relation to SCISA. As such, the OPC has, in the context of advice to Parliament on reforming the *Privacy Act*, recommended that the obligation to conduct PIAs be elevated to a legal requirement rather than a policy one.<sup>15</sup> This is equally applicable in the context of the proposed reform to Canada's national security legal framework.

#### **(VI) RECORD KEEPING**

Our detailed views on accountability appear elsewhere in this document, but at this juncture it should be stated that record-keeping is an essential prior condition to effective review. The OPC's advice to Public Safety in the context of the SCISA Deskbook was clear on this point: it called for guidance on the content of records that should be kept, including a description of the information shared and the rationale for disclosure.

#### **(VII) DOMESTIC INFORMATION SHARING UNDER OTHER LAWFUL AUTHORITIES**

Finally, SCISA is not the only mechanism by which information-sharing for national security purposes takes place.<sup>16</sup> In principle, we are of the view that the safeguards, in particular necessity and proportionality, which the OPC recommended in its review of SCISA should apply to all domestic information sharing.<sup>17</sup> As noted above, under EU jurisprudence and principles of international law, in a democratic society, intrusive state measures need to be rigorously justified as being both necessary and proportionate.<sup>18</sup>

#### ***International Information Sharing***

One of the most important lessons learned from Canada's anti-terrorism efforts since 9/11 has been that international information sharing can lead to serious human rights abuses, including torture. The existing legal framework must be clarified to reduce these risks to a minimum and

.../9

<sup>14</sup> Treasury Board of Canada Secretariat, *Directive on Privacy Impact Assessment*, effective April 2010. <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308>

<sup>15</sup> *Privacy Act Reform in an Era of Change and Transparency: recommendation 7* ([https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl\\_sub\\_160322/#toc1\\_2d](https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_160322/#toc1_2d))

<sup>16</sup> Cohen, Stanley, "National Security Information Sharing", Chapter 8 from *Privacy, Crime and Terror — Legal Rights and Security in a Time of Peril* (Butterworths, 2005)

<sup>17</sup> OPC, "C-51 and surveillance," Chapter 2 from *2015-2016 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act* (Sept. 2016) –

([https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201516/ar\\_201516/#heading-0-0-4](https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201516/ar_201516/#heading-0-0-4))

<sup>18</sup> See footnote 10.

must consider the fact that once information is shared with foreign states, Canada has lost control of that information. In the OPC's submission to the Senate Standing Committee on National Security and Defence on Bill C-44, *An Act to amend the Canadian Security Intelligence Service Act and other Acts*<sup>19</sup> on March 9, 2015, it cited the Supreme Court of Canada decision in *Wakeling v. United States of America*<sup>20</sup> which confirmed the importance of accountability and oversight measures to safeguard information shared with foreign states. Absent statutory safeguards, the protection of individuals against the risk of mistreatment would depend on the application of general constitutional principles which have not been defined clearly in the context of information sharing amongst national intelligence agencies.

Parliament also has a role in protecting individuals against violations of human rights. We would suggest that any powers conferred on national security agencies must be exercised in a way that respects Canada's obligations under international human rights law in general and, specifically, the Convention Against Torture. Clear statutory rules should be enacted to prevent information sharing from resulting in a violation of Canada's international obligations. We note Justice O'Connor's recommendation that "information should never be provided to a foreign country where there is a credible risk that it will cause or contribute to the use of torture."<sup>21</sup>

In addition, the Governments of Canada and the United States have developed joint privacy principles in support of the *Beyond the Border Action Plan: A Shared Vision for Perimeter Security and Economic Competitiveness*.<sup>22</sup> These principles include reference to ensuring accuracy of information, limiting retention of information collected, ensuring relevance and necessity in the collection of personal information, limiting onward transfer of information to third countries, allowing redress before existing national authorities where a person believes their privacy has been infringed and requiring effective oversight. An issue for consideration is importing some of the principles into law. Our concerns regarding information sharing agreements as articulated above apply equally to international information sharing activities. We would urge that minimum content be defined, and that agreements be reviewed by independent bodies including the OPC.

.../10

---

<sup>19</sup> OPC's statement before the Senate Standing Committee on National Security and Defence (SECD) on Bill C-44, *An Act to amend the Canadian Security Intelligence Service Act and other Act*, March 9, 2015

([https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl\\_20150309/](https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl_20150309/))

<sup>20</sup> 2014 SCC 72.

<sup>21</sup> The recommendation continues: "Policies should include specific directions aimed at eliminating any possible Canadian complicity in torture, avoiding the risk of other human rights abuses and ensuring accountability." *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar*, 2006; recommendation 14, page 345.

<sup>22</sup> *Beyond the Border Action Plan: Joint Statement of Privacy Principles*, June 28, 2012 (<https://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2012/20120628-2-en.aspx>)

### ***Investigative Capabilities in a Digital World***

The Green Paper rightly claims that law enforcement and national security investigators must be able to work as effectively in the digital world as they do in the physical, and that laws governing the collection of evidence have not kept pace with new technologies. However, from these premises one does not proceed to loosen legal rules or lower standards of protection. To the contrary, safeguards which have long been part of our legal traditions must be maintained yet adapted to the realities of modern communication tools, one of which is that these devices hold and transmit extremely sensitive personal information.

A preliminary observation before entering the discussion of metadata: the Green Paper appears to conflate law enforcement and national security agencies, which are two very distinct and separate mechanisms for ensuring public safety. Law enforcement and intelligence agencies have different mandates and work in different environments. Clarity on this is critical since different rules could be adopted for different manners of investigations. Plainly, the context of use for investigative powers matters a great deal to the privacy of individuals.

#### **(I) METADATA IN A CRIMINAL LAW CONTEXT**

Metadata, generated constantly by digital devices, can be far more revealing than the information on the outside of an envelope or found in a phonebook, as it is commonly characterized. For instance, metadata can reveal medical conditions, religious beliefs, sexual orientation and many other elements of personal information.<sup>23</sup> The British signals intelligence agency, GCHQ, has publicly stated that metadata is more revealing than the content of communications<sup>24</sup>. In short, it can be highly sensitive depending on the context.

Basic subscriber information, which is a form of metadata, is undeniably useful for investigative purposes. The Green Paper suggests it should be available to law enforcement more easily than under current laws because the police, particularly in the early stages of an investigation, do not have enough evidence to be in a position to satisfy a judge that there is reasonable grounds to believe a crime was committed and that the metadata requested would assist in the investigation.

.../11

---

<sup>23</sup> Office of the Privacy Commissioner, *Metadata and Privacy*, 2014. ([https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md\\_201410/](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/))

<sup>24</sup> Daniel Weitzner, who founded the Internet Policy Research Initiative at the Massachusetts Institute of Technology, considers metadata “arguably more revealing [than content] because it’s actually much easier to analyze the patterns in a large universe of metadata and correlate them with real-world events than it is to go through a semantic analysis of all of someone’s email and all of someone’s telephone calls.” (Daniel Weitzner, quoted in E. Nakashima, “Metadata reveals the secrets of social position, company hierarchy, terrorist cells”, *The Washington Post*, June 15, 2013.)

Bill C-13, the *Protecting Canadians from Online Crime Act*, in force since 2015, has already lowered legal thresholds for accessing metadata. Under it, a production order for "transmission data", transaction records and location tracking can be obtained from a judge on a standard of "reasonable grounds to suspect".<sup>25</sup> An order to preserve information or evidence can also be sought on mere suspicion,<sup>26</sup> giving law enforcement more time to find information in order to satisfy a judge on reasonable grounds to believe that an order for the production of the content of communications is warranted. The *Criminal Code* and the Supreme Court of Canada's decision in *Spencer*<sup>27</sup> even allow for collection in exigent circumstances with no court authorization at all.

We have not seen evidence why these provisions do not give law enforcement adequate tools to do their job. The government is proposing to further reduce safeguards. It has a duty to provide precise explanations as to why existing thresholds cannot be met and why administrative authorizations to obtain metadata, rather than judicial authorizations, sufficiently protect Charter rights absent exigent circumstances.

In our view, recent cases of metadata collection show that existing standards should, in fact, be tightened and that privacy protections should be enhanced. The past few years has seen extensive coverage and public concern over the operations of the Communications Security Establishment<sup>28</sup>, CSIS<sup>29</sup>, the RCMP<sup>30</sup>, the Sûreté du Québec and the Montreal Police (SPVM)<sup>31</sup> stemming from the collection, use, retention and disclosure of metadata. In many cases, the collection of metadata, including with warrants, involved innocent individuals who were not suspected of criminal activity or of representing a threat to national security.

.../12

---

<sup>25</sup> Criminal Code of Canada, section 487.016 (<http://laws-lois.justice.gc.ca/eng/acts/C-46/page-109.html> )

<sup>26</sup> Criminal Code of Canada, section 487.013 (<http://laws-lois.justice.gc.ca/eng/acts/C-46/page-109.html> )

<sup>27</sup> R. v. Spencer, 2014 SCC 43, [2014] 2 S.C.R. 212 (<https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do>)

<sup>28</sup> Office of the Communications Security Establishment Commissioner Annual Report 2015-2016, p. 20. (<https://www.ocsec-bccst.gc.ca/s21/s68/d365/eng/highlights-reports-submitted-minister#toc-tm-2>)

<sup>29</sup> CSIS broke law by keeping sensitive metadata, Federal Court rules, November 3, 2016 <http://www.cbc.ca/news/politics/csis-metadata-ruling-1.3835472>; Le SCRS a illégalement conservé des données personnelles, dit la Cour fédérale, November 3, 2016 <http://www.lapresse.ca/actualites/justice-et-affaires-criminelles/actualites-judiciaires/201611/03/01-5037489-le-scrs-a-illegalement-conserve-des-donnees-personnelles-dit-la-cour-federale.php>

<sup>30</sup> Review of the Royal Canadian Mounted Police – Warrantless Access to Subscriber Information [https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201314/201314\\_pa/#heading-0-0-4](https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201314/201314_pa/#heading-0-0-4)

<sup>31</sup> La SQ a espionné six journalistes: Le ministre de la Sécurité publique ordonne une enquête administrative, le 3 novembre, 2016, <http://www.ledevoir.com/societe/medias/483697/six-journalistes-surveilles-par-la-sq>  
Quebec to hold public inquiry into police surveillance of journalists, November 3, 2016 <http://www.theglobeandmail.com/news/national/quebec-to-hold-public-inquiry-into-surveillance-of-journalists/article32657198/>

A modernized law adapted to new technologies must take into consideration the fact that metadata emitted by digital devices can reveal personal information whose sensitivity often exceeds that for which warrants have traditionally been required in the pre-digital world. It must also ensure that the state's modern investigative tools do not violate the privacy of law abiding citizens.

First and foremost, it is important to maintain the role of judges in the authorization of warrants for the collection of metadata by law enforcement. Despite its imperfections, the judicial system ensures the necessary independence for the protection of human rights.

But we also now know that it is probably not enough to rely solely on the judiciary. Indeed, some judges have made this point themselves. In a recent ruling<sup>32</sup>, Ontario Superior Court Justice John Sproat found he did not have the power to impose privacy protective conditions on a production order involving the metadata of thousands of individuals who happened to be within the vicinity of a number of crimes. He said this responsibility rests with legislators.

We also believe that it is incumbent on Parliament to better define the conditions under which the sensitive metadata of Canadians should be available to police forces. These conditions include adopting sufficiently high legal thresholds and criteria for the issuance of court orders, but also, where these criteria are met, adding limitations to protect the privacy of people who are incidentally targeted by a warrant but are not suspected of involvement in a crime.

The criteria precedent to the issuance of orders would include but may not be limited to the burden of proof (suspicion or belief). On the whole, these criteria should provide law enforcement access to metadata where necessary to pursue their investigations but only in a way that recognizes the often sensitive nature of this type of information. For example, it could be prescribed that the collection of metadata should be a last resort, after all other investigative methods have been exhausted. This is already a condition for access to the content of communications and, as stated, metadata can be more sensitive in nature. Similarly, this type of surveillance could be limited to serious crimes to be prescribed in legislation, for instance crimes of violence where public safety interests may outweigh potential risks to privacy.

In cases where those pre-conditions are met, the law should then add conditions to protect the privacy of people who are incidentally targeted by a warrant but are not suspected of involvement in a crime. Judges could also be authorized to issue case specific limitations, where warranted. For example, there could be restrictions on use and disclosure (only for the

.../13

---

<sup>32</sup> R. v Rogers Communications, 2016 ONSC 70.

investigation of the crime for which the authorization is granted) and limits on retention (metadata related to communications that have no connection with criminal activity should be destroyed without delay).

## (II) RETENTION

The Green Paper also suggests facilitating police investigations by adopting in law general data retention requirements which would prevent companies from deleting their customers' data before law enforcement can seek production orders. We note that in 2014, the European Court of Justice (ECJ) issued a decision<sup>33</sup> invalidating the 2006 EU Data Retention Directive,<sup>34</sup> largely on the basis that it entailed a significant interference with Europeans' fundamental rights without imposing sufficient limitations on law enforcement's use of the information collected. While the ECJ recognized that the objective of fighting terrorism and serious crime was legitimate, it found that the retention of data for the purpose of possible access by national law enforcement authorities seriously interfered with the right to private life and the protection of personal data, both of which are guaranteed in the Charter of Fundamental Rights ("EU Charter"). Article 52(1) of the EU Charter requires that any limitation on the exercise of guaranteed rights be necessary and proportionate. The ECJ held that the absence of any limit on whose information could be retained or how it could be accessed or used, and the lack of guidance to national authorities in controlling the use of retained data, meant that the Directive entailed "a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what it is strictly necessary."

Preservation demands (to hold information for 21 days) and orders (which preserve information for three months) are a current tool under the *Criminal Code* which can be used. We have not seen evidence why these tools do not work. Introducing a broad retention requirement, not only impedes on human rights, as noted in the ECJ decision, it also increases the risks of breaches to that personal information. Retention requirements, if any, should be scoped narrowly, focussing on serious crime only, and should be for the briefest period of time possible.

.../14

---

<sup>33</sup> The full ECJ judgement: [eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1)

<sup>34</sup> Directive 2006/24/EC: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1480100474890&uri=CELEX:32006L0024>



### (III) METADATA IN A NATIONAL SECURITY CONTEXT

Earlier this year, OCSEC reported on inappropriate information sharing conducted by the Communications Security Establishment (CSE).<sup>35</sup> In short, due to a filtering technique that became defective, metadata was not being properly minimized (for example, it was not removed, altered, masked or otherwise rendered unidentifiable) before being shared with international “Five Eyes” partners—the signals intelligence agencies of Australia, New Zealand, the United Kingdom and the United States. As noted in our subsequent report<sup>36</sup>, CSE shared large volumes of metadata with its international partners, some of which may have had a “Canadian privacy interest.”

The OPC made several recommendations following its investigation into the matter, including that CSE conduct a PIA on their metadata program and that the *National Defence Act* be amended not only to clarify the CSE’s powers but that those powers be accompanied by specific legal safeguards with respect to collection, use and disclosure in order to protect the privacy of Canadians. While the government maintains that metadata is essential for identifying threats, this case demonstrates that CSE activities related to metadata can affect the privacy of a large number of Canadians, and that these activities should be governed by appropriate legal safeguards.

In another recent case, the Federal Court found that CSIS had unlawfully retained for an extended period metadata that was not “strictly necessary” to its mandate related to threats to national security.<sup>37</sup> In our view, the law should be amended to ensure that where the personal information of individuals who are not suspected of terrorism is obtained incidentally to the collection of information about threats, the former should be destroyed once it has been determined after analysis that individuals have been cleared of any suspected terrorist activities.

### (IV) INTERCEPTION AND ENCRYPTION

#### *Context*

Encryption represents a particularly difficult dilemma. As the Green Paper sets out in its scenarios, encryption can be a significant obstacle to lawful investigations and even to the

.../15

---

<sup>35</sup> Office of the Communications Security Establishment Commissioner Annual Report 2015-2016, p. 20. (<https://www.ocsec-bccst.gc.ca/s21/s68/d365/eng/highlights-reports-submitted-minister#toc-tm-2>)

<sup>36</sup> The OPC’s 2015-2016 Annual Report to Parliament on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act*: Chapter 2: C-51 and surveillance ([https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201516/ar\\_201516/#heading-0-0-4](https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201516/ar_201516/#heading-0-0-4))

<sup>37</sup> Federal Court of Canada, *In the Matter of An Application by X for Warrants ...*, 2016 FC 1105 ([http://cas-cdc-ww02.cas-satj.gc.ca/rss/DES%20\(warrant\)%20nov-3-2016%20public%20judgment%20FINAL%20\(ENG\).pdf](http://cas-cdc-ww02.cas-satj.gc.ca/rss/DES%20(warrant)%20nov-3-2016%20public%20judgment%20FINAL%20(ENG).pdf))

enforcement of judicial orders. As a legal matter, individuals who use it and companies that offer it to their customers are subject to laws and judicial warrants, and these sometimes require access to personal information where legitimately needed in cases where public safety is at risk. On the other hand, as a technological tool, encryption is extremely important, even essential, for the protection of personal information and for the security of electronic devices in use in the digital economy. Unfortunately, the crux of the problem springs from the fact there is no known way to give systemic access to government without simultaneously creating an important risk to the security of this data for the population at large. Laws should not ignore this technological fact.

For contextual purposes, it is useful to distinguish between three primary modes of encryption: (1) traditional, which routinely is applied to systems and infrastructure (e.g. internal e-mail or telecommunications networks), where service providers typically hold the cryptographic key, (2) end-device encryption, such as that found on certain handheld devices and computers, where some service providers hold the key, while other firms do not, and, (3) third-party encryption software or applications (end-to-end encryption) which consumers can freely download to their devices, and where typically only the users control the key. It is the second and third encryption scenarios that pose more challenges in terms of how to address the needs of law enforcement.

### *International approaches*

We fully understand the importance of encryption for a wide range of stakeholders – industry, civil society, citizens and police – who all have an interest in the issue. Cryptographic protections are important for online trust, e-commerce and general privacy protections. Therefore, it is not solely a law enforcement or security issue, with which many jurisdictions continue to grapple with options and regulations.

One instructive case for policy makers to bear in mind was a US law from two decades ago which mandated specific technical intercept requirements (the *Communications Assistance for Law Enforcement Act*). During implementation, in subsequent audits and reports to Congress, it was noted that there were serious cost overruns, administrative difficulties given technical complexities and legal problems stemming from enforcing compliance via inspections.<sup>38</sup> Many technical experts also have noted since that the specifics of the law were soon after overshadowed by changes in technology, network architecture and prevalence of social media.

Other countries legislating in this domain have sought to avoid many of those risks through more flexible regulatory approaches or more principle-base, tech-neutral law. For example, in

.../16

---

<sup>38</sup> Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation (<https://oig.justice.gov/reports/FBI/a0419/index.htm>)

recent years EU states have taken distinct and differing approaches in policy and law, either ruling out backdoor requirements as too great a risk for data protection and security (the Netherlands), opting to legislate specific powers for investigative orders where encryption is encountered - backed by heavy fines (France), or requiring plaintext from companies pursuant to court orders (the UK). These laws were fiercely debated and met with mixed results.

One factor that greatly impedes the efficacy of such laws is that many encryption tools originate from sources and firms abroad and are widely available, including to criminals and terrorists, so would restrictions primarily affect ordinary citizens with limited knowledge of protection tools? The rapid pace of technological change is also an important issue.

### ***Existing Canadian rules***

It should be noted that Canada is not without rules which may assist law enforcement agencies in addressing encryption issues. For instance, assistance order provisions came into force in March 2015 with the *Protecting Canadians from Online Crime Act*. That legislation empowers a judge to attach an assistance order<sup>39</sup> to any search warrant, interception order, production order or other form of electronic surveillance. These orders compel any named person to help “give effect” to the authorization, and these have been used in investigations to defeat security features or compel decryption keys.<sup>40</sup> The requirements are backed with serious fines and/or criminal penalties. In the US, companies respond to such orders thousands of times a year, as noted in transparency reporting.<sup>41</sup> However, the use of these orders to compel individuals to hand over the encryption codes that they use on their devices raises the possibility of self-incrimination and therefore *Charter* issues.

It is also important to note that at the federal level, provisions already exist for telecommunications carriers to build in surveillance capability, retain communications metadata and provide decrypted content to government upon request.<sup>42</sup> If these requirements (the *Solicitor-*

.../17

---

<sup>39</sup> Section 487.02 of the *Criminal Code* (<http://laws-lois.justice.gc.ca/eng/acts/C-46/page-111.html> )

<sup>40</sup> Clayton Rice, “Apple and ‘Assistance Orders’ in Canada” (Nov. 8, 2015) <http://www.claytonrice.com/apple-and-assistance-orders-in-canada/>; Justin Ling and Jordan Pearson, “Canadian Police Obtained BlackBerry’s Global Decryption Key”, April 12, 2016 (<https://news.vice.com/article/exclusive-canada-police-obtained-blackberrys-global-decryption-key-how>)

<sup>41</sup> Apple, *Report on Government Information Requests*; July 1 - December 31, 2013; (<http://images.apple.com/ca/privacy/docs/government-information-requests-20131231.pdf>)

<sup>42</sup> Public Safety Canada, SGES, standard 12, Page 6 (2008).

*General Enforcement Standards* [SGES]<sup>43</sup>), which have been a condition of licensing since the mid-1990s<sup>44</sup> are not being properly implemented or enforced, government needs to explain exactly where these standards fall short and why they need modification.

### ***Possible solutions***

Parliament should proceed cautiously before attempting to legislate solutions in this complex area. Given the experience and factors noted, we believe it preferable to explore the realm of technical solutions which might support discrete, lawfully authorized access to specific encrypted devices, as opposed to imposing general legislative requirements. At the same time, an open dialogue with the technical community, industry, civil society and privacy experts including the OPC, could provide valuable input; the Green Paper could be the beginning of such a dialogue.

However, if the government feels that a legislative solution is required, we believe that amendments should reflect and articulate the principles of necessity and proportionality<sup>45</sup>, so as to narrow how much information is decrypted, and that such extraordinary measures should be used as a last resort.

### **(V) TRANSPARENCY REPORTING**

Another aspect missing from the Green Paper concerns transparency reporting, which is an important part of ensuring balance and accountability. Since 2009, the OPC has advocated for a reporting regime on personal information disclosures to government by commercial organizations. The OPC has addressed these calls to Parliament, government bodies, companies and industry associations. Its 2013 PIPEDA Reform paper called for a reporting regime to be enacted, as did the Office's recommendations to Parliament on Bill S-4, the *Digital Privacy Act* in 2014-2015.<sup>46</sup> These recommendations call upon commercial organizations to be open about the number, frequency and type of lawful access requests they respond to.

.../18

---

<sup>43</sup> Duncan Campbell, "Intercepting the Internet", *The Guardian*, April 29, 1999. (<http://www.theguardian.com/technology/1999/apr/29/onlinesupplement3>)

<sup>44</sup> These are jointly overseen and administered by Public Safety Canada, Innovation Science and Economic Development (ISED) and Canadian Radio and Telecommunications Commission.

<sup>45</sup> Christopher Kuner, "Encryption and the rule of law" 38th Annual Conference of Data Protection and Privacy Commissioners (Marrakech, Morocco), p. 3. (<https://icdppc.org/wp-content/uploads/2015/03/Dr-Christopher-Kuner.pdf>)

<sup>46</sup> Bill S-4, An Act to amend the *Personal Information Protection and Electronic Documents Act* and to make a consequential amendment to another Act (the *Digital Privacy Act*), the OPC's Submission to the Standing Committee on Industry, Science and Technology, March 11, 2015.

In the past few years, six telecommunications companies (Rogers, TELUS, TekSavvy, MTS Allstream, Sasktel and Wind) in Canada each began to publish annual reports which provide statistical details on various forms of customer name/address checks by government, court orders and warrants, as well as emergency requests from police in life threatening situations. These categories are generally described in the reports with specific examples, as well as a description of the applicable legal authorities involved. With the OPC's assistance, the Department of Innovation, Science and Economic Development has provided an additional set of guidelines to encourage consistent reporting.

Transparency reporting limited to the private sector is insufficient and it is frankly abnormal that government institutions are not legally required to report on these issues, subject of course to limitations required to protect investigative methods. The OPC has therefore recommended strengthening reporting requirements on broader privacy issues dealt with by federal organizations as well as specific transparency requirements for lawful access requests made by agencies involved in law enforcement. There are various models and approaches for developing such reporting. On the public sector side for example, the *Annual Report on the Use of Electronic Surveillance* tabled annually in Parliament since 1977 (pursuant to Criminal Code section 195) has provided a reporting framework on transparency for very sensitive law enforcement investigations.

Timely, accurate statistical information on government requests and access of personal information – in the form of clear transparency reports at regular intervals – can form the basis for rational consumer choices and build citizen confidence in a growing digital economy and its interface with the state for law enforcement and security purposes. Public debates and decisions on privacy need grounding in facts and legal reality. Good transparency reporting based on evidence can support these discussions.

### ***Conclusion***

This exercise stems from a government commitment to repeal the problematic elements of Bill C-51, the *Anti-terrorism Act, 2015*, a commitment whose objective was to strike a better balance between security and human rights. As stated at the outset, we support the broader approach under which the entire security framework is to be reviewed, because problematic elements of this framework are not all found in Bill C-51. For instance, commissions of inquiry were conducted to review national security activities in the aftermath of 9/11 and have concluded that Canada had violated fundamental rights.

Now that it is clear the government wishes to take this opportunity to consider new state powers, we feel it is important that we not forget the lessons of history. One of these lessons is that once conferred, new state powers are rarely relinquished. While we applaud the government's wish to reconsider recent amendments with a view to strengthening human rights

- 19 -

protections, we trust this same philosophy will apply to the potential expansion of investigative tools. Government should only propose and Parliament should only approve such expansion if it is demonstrated to be necessary, not merely useful or convenient, and proportionate. For its part, proportionality will depend on the adoption of strong and effective legal safeguards, standards and oversight.

This consultative exercise is a positive step, and we welcome the opportunity to continue the discussion about how best to ensure that Canada's national security framework truly protects Canadians and their privacy.

Sincerely,

A handwritten signature in black ink, appearing to read 'D. Therrien', with a stylized flourish at the end.

Daniel Therrien  
Privacy Commissioner of Canada

.../20



Drew McArthur  
Acting Information and Privacy  
Commissioner for British  
Columbia



Jill Clayton  
Information and Privacy  
Commissioner of Alberta



Ronald J. Kruzeniski, QC  
Information and Privacy  
Commissioner of Saskatchewan



Charlene Paquin, Ombudsman  
Manitoba



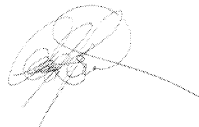
Brian Beamish  
Information and Privacy  
Commissioner of Ontario



M° Jean Chartier  
President  
Commission d'accès à  
l'information du Québec



Catherine Tully  
Information and Privacy  
Commissioner for Nova Scotia



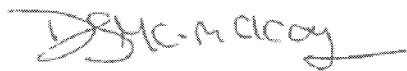
Anne E. Bertrand, Q.C.  
Access to Information and  
Privacy Commissioner  
New Brunswick



Donovan Molloy, QC,  
Information and Privacy  
Commissioner  
Office of the Information and  
Privacy Commissioner for  
Newfoundland and Labrador



Karen A. Rose  
Information and Privacy  
Commissioner of Prince Edward  
Island



Diane McLeod-McKay  
Yukon Information and Privacy  
Commissioner

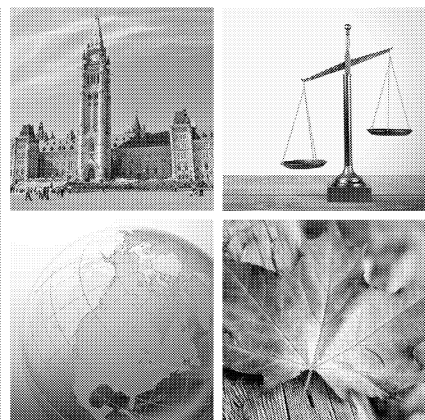


Elaine Keenan-Bengts, LL.B.,  
B.A.  
Information and Privacy  
Commissioner of Nunavut and  
the Northwest Territories

# Our Security, Our Rights

## National Security Green Paper, 2016

### Background Document



This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.



Government  
of Canada

Gouvernement  
du Canada

Canada





*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

# Our Security, Our Rights: National Security Green Paper, 2016

---

*BACKGROUND DOCUMENT*

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## CONTENTS

Introduction .....	5
Accountability .....	9
Prevention.....	15
Threat Reduction .....	21
Domestic National Security Information Sharing.....	26
The Passenger Protect Program .....	33
<i>Criminal Code</i> Terrorism Measures.....	38
Procedures for Listing Terrorist Entities .....	47
Terrorist Financing .....	51
Investigative Capabilities in a Digital World .....	55
Intelligence and Evidence .....	65
Conclusion .....	72
Annex – Diagram of Scenario Characters.....	73

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## INTRODUCTION

### Setting the Scene

Canada has long dealt with terrorism threats from a diverse set of groups. Some threats resulted in tragic terrorist attacks. For example, a terrorist bomb exploded aboard Air India Flight 182 in 1985, killing 329 passengers and crew. In a related incident, a second bomb exploded at Narita airport in Japan, killing two more individuals. This remains the worst terrorist attack in Canadian history.

Following the September 11, 2001 attacks in the United States (U.S.), Canada enacted the *Anti-terrorism Act*. The Act recognized the unique nature of terrorism and created offences addressing specific aspects of terrorism. These offences included contributing to the activities of a terrorist group, instructing someone to carry out a terrorist activity, and harbouring a terrorist.

Since 2001, threats to Canadian and international security have continued to evolve. Groups inspired by al-Qaida have emerged in many parts of the world. In early 2014, one of these groups, al-Qaida in Iraq, severed ties with al-Qaida and emerged anew as the Islamic State of Iraq and the Levant (ISIL). What has been referred to as ISIL will be referred to as Daesh in this document. Since the start of the Syrian conflict in 2011, many Canadians have travelled to Syria and Iraq to join Daesh's predecessor and then Daesh itself. Daesh's declaration of a "caliphate" led to even more of these "extremist travellers" from Canada joining Daesh abroad. Some later returned to Canada, leaving trained and connected terrorist actors in our presence. The return of travellers can result in the presence of trained and connected terrorist actors within Canada.

Extremist narratives have also inspired some Canadians to plot and pursue attacks. Sometimes their targets are domestic, such as the 2014 attacks in Ottawa and Saint-Jean-sur-Richelieu. Other times, their targets are outside Canada, such as the Algerian gas plant attacked by terrorists, including two Canadians, in 2013.

The Minister of Public Safety and Emergency Preparedness recently released the *2016 Public Report on the Terrorist Threat to Canada*. The Report noted that the principal terrorist threat to Canada remains that posed by violent extremists who could be inspired to carry out an attack within Canada. Violent extremist ideologies espoused by terrorist groups like Daesh and al-Qaida continue to appeal to certain individuals in Canada.

Both the threat of terrorism and the counter-terrorism tools we use to respond have evolved over the years. However, there has been one constant imperative from the Government of Canada's perspective. That is to ensure that any actions by the Government respect Canadian values, including the rights and freedoms guaranteed by the *Charter*, as well as equality and multiculturalism.

National security institutions in Canada are professional, responsible and effective in the work they do. They work within a well-defined set of legal authorities and respect Canadian law. Their core

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

duty is to keep Canadians safe—and they do so daily. National security institutions in Canada are subject to measures that make them accountable. These accountability measures ensure that these institutions are acting within the law and are being effective. Accountability for national security institutions is, therefore, an important part of any discussion on national security, as it offers protections and safeguards.

The Government is aware that its actions in security matters can impact rights. In protecting national security, the Government must find an appropriate balance between the actions it takes to keep Canadians safe and the impact of those actions on the rights we cherish. The question is: what is an appropriate and reasonable impact?

The Canadian public, stakeholders, experts and those in government institutions will have a variety of views on what constitutes an appropriate balance. Canadians rightly expect strong justifications to limits their rights. This means that we must look at measures to protect national security to see whether they are effective, if there are potential alternatives and if they have properly taken into account the rights they affect.

## Human Rights

Canada is founded upon the rule of law, of which the Constitution is the “supreme law.” This means that all laws enacted by Parliament and all actions taken by the Government of Canada must be consistent with the Constitution, which includes the *Charter*. The *Charter* reflects our basic values and guarantees our fundamental rights and freedoms, including freedom of expression and association, and the rights to equality, privacy, and the presumption of innocence. The purpose of the *Charter* is to ensure that we are governed in accordance with our basic values. Any laws of Parliament and actions of government that are inconsistent with the *Charter* are unconstitutional and can be declared so by the courts.

The rights and freedoms guaranteed in the *Charter* are not absolute. They can be limited in accordance with the law, if justifiable. Justifiable limitations are generally those that pursue important objectives and that impact rights or freedoms as little as reasonably possible in the circumstances. Also, limitations are only justifiable if, overall, the benefits from these limitations outweigh the harm to the right.

This concern for balance is acutely important in the national security context, where *Charter* rights and freedoms regularly come into play. Measures to protect national security are aimed at fulfilling the Government's primary mandate, which is to safeguard the people, institutions and values of Canada. Preserving national security includes protecting what defines Canada, including democracy, multiculturalism, and respect for the rule of law and fundamental rights and freedoms.

The *Charter* establishes a minimum standard of conduct by governments in Canada. Governments are free to produce legislation or policies, or carry out activities, that give greater protection to rights

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

and freedoms than the *Charter* requires. In some cases, the appropriate balance between national security concerns and *Charter* rights may result in greater protection. The Government is interested in the views of Canadians about when it may be appropriate in national security matters to give greater protection to rights and freedoms than that required by the *Charter*.

## Privacy

In recent years, many countries have experienced high-profile public controversies about privacy impacts of national security activities.

It is difficult to hold an informed public debate about whether privacy impacts are appropriate. In part, this is because revealing some details about national security operations can undermine their effectiveness.

That said, effective and sustainable anti-terrorism measures should reflect a robust democratic consensus, at least at the level of principles. In matters involving privacy in particular, it might not be enough to achieve that consensus if anti-terrorism activities merely satisfy the minimum constitutional and legal standards. The Government is interested in the views of Canadians to help determine where the consensus lies.

## Consultation Process

How best to respond to terrorism while protecting rights and freedoms is a highly complex issue. As the Government examines possible changes to Canada's counter-terrorism framework, it is asking Canadians to become active partners in finding an appropriate balance between security and rights. These consultations will help the Government develop more informed policies in this complex area.

Each chapter of this background document provides information on applicable laws, issues, challenges and potential impacts on rights in the counter-terrorism context. It contains hypothetical scenarios to better illustrate the concepts being presented.

All Canadians are invited to respond online at **[Canada.ca/national-security-consultation](http://Canada.ca/national-security-consultation)** to the issues raised in the Green Paper and this background document. Responses will be accepted until December 1, 2016.

The Government will consider the responses and use them to help develop any new laws and policies. The Government will also keep Canadians up to date on the progress of consultations.

Hypothetical scenarios will be presented throughout this document to illustrate issues. The roles of the characters used in these scenarios are set out in the Annex.



*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

*Our main scenario starts as follows...*

Mr. A is a charismatic speaker who holds weekly meetings in a local community centre. He has strong views on social and political issues. He invites individuals with similar interests to attend. Some of these individuals have become friends with each other, and with Mr. A. They are also his most devoted followers.

Mr. A believes that things in Canada need to change. He is looking for people who are willing to get involved and make this happen. Over time, his calls for political and social change start taking on a more violent tone.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## ACCOUNTABILITY

Some government agencies have unique intelligence collection and enforcement powers to protect national security. They must exercise these powers according to specific laws and in a manner consistent with the *Charter*. These powers are potentially intrusive, and can impact rights and freedoms. For this reason, these powers must be exercised with great care.

Much work of these agencies occurs in secret. This is because the public disclosure of sensitive information could harm national security by putting investigations, sources of information and investigative techniques at risk. As a result, effective accountability mechanisms are key to maintaining the public's trust in these agencies. Accountability mechanisms provide assurance that agencies act responsibly, strictly within the law and with respect for Canadians' rights and freedoms.

### Ministerial Oversight

The Minister of Public Safety and Emergency Preparedness and the Minister of National Defence have important responsibilities with regard to the national security and intelligence agencies in their respective portfolios.

The Minister of Public Safety and Emergency Preparedness is responsible for three national security agencies: the Canada Border Services Agency (CBSA), CSIS and the Royal Canadian Mounted Police (RCMP). The Minister is also responsible for Public Safety Canada.

The Minister of National Defence is responsible for the Communications Security Establishment (CSE), the Department of National Defence (DND) and the Canadian Armed Forces (CAF).

The Ministers are accountable to Parliament for the activities of their respective agencies.

If the activities of CSE or of CSIS employees are believed to have contravened the law, the minister responsible for the relevant agency is engaged and the Attorney General of Canada is informed.<sup>1</sup>

Ministers can issue formal directions that establish guidelines on the conduct and management of operations, although the principle of police independence limits direct ministerial involvement in day-to-day law enforcement operations. Ministerial Directions (MDs) may also specify reporting requirements and procedures for obtaining approval for agency activities.

A number of MDs are currently in effect for the CBSA, CSE, CSIS and the RCMP. For example, in 2015, CSIS was issued wide-ranging new MD on operations and accountability. The RCMP is also

---

<sup>1</sup> In the case of CSE, it is the CSE Commissioner who informs the Minister and Attorney General of Canada. Reports to the Attorney General of Canada about CSIS employees must also be provided to the Security Intelligence Review Committee.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

subject to several MDs that provide guidance on aspects of national security investigations related to sensitive sectors, accountability, and cooperation. MDs on information sharing with foreign entities have also been issued to the CBSA, CSE, CSIS and the RCMP. These MDs established a consistent process for deciding whether to share information with foreign entities where there may be a risk of mistreatment stemming from the sharing of information, in accordance with Canada's laws and legal obligations.

## The Judiciary

Courts are involved in national security matters in several ways. Judges decide whether to issue warrants for CSIS and law enforcement agencies to use intrusive powers when investigating threats. Judges ensure that agencies meet the legal requirements to obtain warrants and that the warrants comply with the *Charter*. Judges also have the discretion to include in warrants any terms and conditions that are advisable in the public interest. For example, a judge might limit how long a government institution can keep the information it obtains.

More generally, judges decide whether activities leading to an individual's arrest and criminal prosecution are justifiable and proper. For example, judges examine whether investigators respected constitutional rights during investigations and whether evidence was properly collected and should be admitted at trial. Judges also have the authority to provide remedies to citizens who show law enforcement misconduct.

The Federal Court may also hear applications for judicial review of administrative decisions made by the Government in national security matters. Judicial review is a process by which the courts ensure that government decisions were fair and complied with the law. For example, the Court could review decisions made under national security programs such as the Passenger Protect Program.

## Independent Review

Canada has a long-standing system of independent, non-partisan bodies reviewing the activities of certain agencies that deal with national security matters. Review bodies operate at arm's-length from government. Their main task is to ensure that national security and intelligence agencies comply with the law and MDs.

At present, there are three such bodies:

- the Civilian Review and Complaints Commission (CRCC), responsible for reviewing RCMP activities;
- the Security Intelligence Review Committee (SIRC), responsible for reviewing CSIS activities; and

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

- the Office of the Communications Security Establishment Commissioner (OCSEC), responsible for reviewing CSE activities.

Governor-in-Council (Cabinet) appointees head the CRCC and SIRC. The Governor-in-Council appoints a supernumerary judge or retired judge of a superior court to head OCSEC. Each review body has an independent research staff and legal counsel to help it.

All three review bodies have a mandate to review the activities of, and hear complaints against, the particular agency for which they are responsible. They have access to information held by the agency. Each review body produces a public report every year summarizing its activities, including findings and recommendations from reviews and complaints.

The authority of these three review bodies does not extend beyond the specific agency for which each review body is responsible. As a result, review bodies do not share classified information with each other or conduct joint reviews of national security and intelligence activities.

## Parliament

Parliament has several roles in national security matters. It holds ministers to account for the actions of the institutions for which they are responsible. Parliament reviews, refines and enacts proposed legislation on national security matters. This process often involves calling witnesses to provide expert evidence about the issues raised by the proposed legislation.

Some laws contain provisions requiring a review of the law after a set period. For example, the Government has made a commitment to require a review of the ATA, 2015 after three years. Some laws might also require that a provision expires on a set date unless renewed. Other laws may require an annual report about the use of a particular provision.

House of Commons and Senate committees can also examine national security policy issues and conduct studies of government activities and existing legislation.

Normally, however, parliamentarians do not see classified information. This limits their ability to examine national security issues in depth. To resolve this, the Government has tabled a Bill C-22, the *National Security and Intelligence Committee of Parliamentarians Act*<sup>2</sup> to create a national security and intelligence committee of parliamentarians with broad access to classified information. The committee would examine how institutions are working together to keep Canadians safe from national security threats. It would also seek to ensure that institutions comply with Canada's laws and respect fundamental values, the democratic nature of our open society and the rights and freedoms of Canadians.

---

<sup>2</sup> Bill C-22 can be accessed at:

<http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=8375614>

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## Agents of Parliament

Certain agents of Parliament scrutinize the national security activities of all federal institutions in relation to their specific mandates. For example, the Privacy Commissioner of Canada can examine their handling of personal information. The Privacy Commissioner also has a mandate to review the operations of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) every two years. The Information Commissioner of Canada investigates complaints about the Government's handling of access to information requests. The Auditor General (AG) can conduct "value-for-money" audits of national security programs.<sup>3</sup>

## Commissions of Inquiry

Commissions of inquiry provide another means to keep government institutions accountable. Commissions of inquiry are "established by the Governor in Council (Cabinet) to fully and impartially investigate issues of national importance."<sup>4</sup> Within the last decade, the O'Connor, Iacobucci and Major Commissions<sup>5</sup> each reported on the activities of various national security institutions. Many, but not all, of their recommendations have been implemented. For example, Commissioner O'Connor made a number of detailed recommendations for changes to the framework for national security accountability in Canada that have not been implemented.

---

<sup>3</sup> For example, in spring 2013, the AG reported on its audit of government spending on the Public Security and Anti-Terrorism Initiative; in fall 2012, the AG reported on the Government's efforts to protect Canadian critical infrastructure against cyber threats; and in March 2009, the AG reported on intelligence and information sharing in relation to national security.

<sup>4</sup> Privy Council Office, Commissions of Inquiry.

<sup>5</sup> Specifically, the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (report released September 18, 2006); the Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin (report released 22 October 2008); and the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (report released 17 June 2010).

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## What are other countries doing?

Some of our closest allies, including Australia and the United Kingdom (UK), share democratic traditions and institutions. As such, their experiences ensuring the accountability of national security and intelligence services are useful to consider when reflecting on Canada's own accountability mechanisms.

For instance, both Australia and the UK have parliamentary committees with access to classified information dedicated to national security. Indeed, the UK's Intelligence and Security Committee can, with the government's consent, review specific national security operations.

Australia and the UK also take different approaches to independent review of national security activities. In the UK, a number of different commissioners concentrate on a specific aspect of national security and intelligence across a range of agencies. These include:

- The Interception of Communications Commissioner ensures the propriety of communications interception activities;
- The Intelligence Service Commissioner's Office and the Office of Surveillance Commissioners review covert surveillance activities other than communications intercepts; and
- The Investigatory Powers Tribunal hears complaints and can authorize compensation and other redress.

The UK's system may change shortly, however; the *Investigatory Powers Bill*, currently before the UK Parliament, would consolidate the current bodies into a single Investigatory Powers Commission, and would also establish Judicial Commissioners charged with approving warrants.

Australia, for its part, has long had a consolidated model. There, the Inspector General of Intelligence and Security reviews all key intelligence and security agencies for compliance with the law, ministerial directives, and in regard to human rights.

In addition to its commissions and tribunals, the UK's Independent Reviewer of Terrorism Legislation provides expert commentary on proposed legislation, and reviews the use of powers granted by certain key pieces of existing legislation. In carrying out these duties, the Reviewer – who is appointed from outside of government – has access to classified information. Australia has a similar mechanism, the Independent National Security Legislation Monitor, which reviews, on an ongoing basis, national security and counter-terrorism legislation.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## What do you think?

Should existing review bodies – CRCC, OCSEC and SIRC – have greater capacity to review and investigate complaints against their respective agencies?

Should the existing review bodies be permitted to collaborate on reviews?

Should the Government introduce independent review mechanisms of other departments and agencies that have national security responsibilities, such as the CBSA?

The proposed committee of parliamentarians will have a broad mandate to examine the national security and intelligence activities of all departments and agencies. In addition to this, is there a need for an independent review body to look at national security activities across government, as Commissioner O'Connor recommended?

The Government has made a commitment to require a statutory review of the ATA, 2015 after three years. Are other measures needed to increase parliamentary accountability for this legislation?

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## PREVENTION

A new phrase has appeared in the Canadian lexicon: radicalization to violence. Radicalization to violence is a process where people take up an ideological position that moves them towards extremism and ultimately, terrorist activity.

Semantics are important here. It is not a crime to be a radical. Throughout history, change has been brought about by individuals whose radical ideas have inspired new ways of thinking. What is a crime is terrorism – violence committed in the name of radical ideologies or beliefs. As a Government, as a society, we are obliged to respond to criminal violence, whatever form it takes.

When someone decides to use violence to reach a political, ideological or religious goal, they have “radicalized to violence.” This is where terrorism takes root. This person may be formally linked to a terrorist group, inspired by a terrorist group, or radicalized to violence through their own beliefs. The question is, how does radicalization to violence begin? And, more important, what can be done to prevent it?

### What Plays a Role?

We know that specific “narratives” drive radicalization to violence. These narratives reduce an individual’s understanding of global events to a few simplistic propositions. Radicalization is also a social process occurring within networks and communities, both virtual and physical. People can be influenced by friends, mentors and other individuals in their lives.

Associating with others ascribing to violent radical ideologies can influence individuals to move further down the path of radicalization to violence. For example, it is no accident that many people who become extremist travellers – individuals who go abroad to join or contribute to terrorist groups – know others like them who have gone abroad. Some extremist travellers who return to Canada have the experience to plan and carry out terrorist attacks at home, as well as the credibility to recruit, encourage, mentor and facilitate the actions of aspiring terrorists.

The Internet also plays an important role in radicalization to violence. Terrorist groups use websites, chat rooms and social media as key propaganda and recruitment tools. For example, in the conflict in Iraq and Syria, some individuals and groups regularly post content and video clips on social media. These online posts boast of battlefield victories and seek to justify terrorist attacks and recruit young people from around the globe to join the fight.



*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

### *Consider a scenario...*

Mr. B is 17 years old and in his final year of high school. He was born and raised in a large suburban area. His neighbours think he is polite and he has no criminal record. Several months ago, a friend encouraged Mr. B to attend weekly discussion group meetings hosted by Mr. A. His charisma, moving speeches about global politics and self-confidence immediately drew in Mr. B. Over time, Mr. A's extremist views and promotion of violence began to resonate with Mr. B.

Between weekly meetings, Mr. B now spends much of his time on the family computer, watching violent videos that Mr. A has posted online. Some friends have noticed changes in Mr. B's behaviour and that he spends more time alone than before. Some teachers have noticed that he is less engaged in the classroom and intolerant of the views of his peers during class discussions. His association with Mr. A worries Mr. B's parents, but their attempts to talk to him about it have failed. They want to know what they can do and where they can go for help to prevent their son from becoming fully committed to a violent radical ideology.

## **What Can be Done?**

All levels of government, communities and other stakeholders must work together to steer at-risk individuals away from radicalization to violence. They also need to give at-risk individuals the support they need to choose an alternative path that reflects Canadian values of peace and acceptance.

Law enforcement organizations play an important role. They seek to support individuals at risk of radicalization to violence and respond if individuals progress to criminal activities. The RCMP train law enforcement officers and front-line personnel to recognize early warning signs and lead interventions to divert individuals from the path of radicalization to violence. As well, Correctional Services Canada conducts tailored interventions for inmates who have radicalized to violence or who are at risk of doing so.

Family members, friends and others close to at-risk individuals can also play a key role in countering radicalization to violence. They are often aware of the individual's beliefs and intentions. Individuals who are early on in the process of radicalization may have many questions and doubts. At this early stage, it may be possible to steer individuals away from radicalization to violence. For this reason, it is essential to support local communities to address this issue.

## **National Leadership**

The Government is also exploring new ideas and innovative approaches to counter radicalization to violence. Budget 2016 announced \$35 million over five years, with \$10 million per year ongoing, to create an Office of the community outreach and counter-radicalization coordinator. The Office will

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

lead Canada's response to radicalization to violence, coordinate federal, provincial, territorial and international initiatives, and support community outreach and research. The material immediately below describes in greater detail what the Office could do.

### *Work with Communities*

The most effective way to prevent radicalization to violence often lies within communities. It involves working with local leaders to develop early intervention programs. A key focus for the new Office is to reach out to Canadians and build constructive relationships with communities across Canada, raise general awareness about threats and means to address them, and maintain a continual dialogue with those communities.

Engaging with Canadians will help identify priorities for the Office and inform the development of a national strategy to counter radicalization to violence. The Office is seeking to support programs that focus on individuals at risk of radicalization to violence. These programs can include community capacity-building, mentorship, multi-agency interventions and training and support for those involved in front-line intervention work (such as youth workers, corrections and parole officers, social service providers, faith leaders and mental health practitioners).

The City of Montreal is also working in this area. It has established a Centre for the Prevention of Radicalization Leading to Violence. The Centre brings together partners from various sectors, including health and social services, public safety and education. The goal is to develop expertise, define areas of prevention and intervention, and empower communities to address radicalization to violence. The Office can incorporate lessons learned from Montreal's experience into future programming.

### *Engage Youth and Women*

Radicalization to violence in Canada affects young people disproportionately. Engaging with youth is therefore important in addressing this issue. Early in the process of radicalization they may have many questions and doubts. They turn to the guidance that is available. At this early stage, tailored outreach has the potential to steer at-risk youth away from radicalization to violence. The Office is looking to start a positive conversation with young people, raise their awareness about the dangers of becoming radicalized to violence, and empower them to respond to the issue.

Women can play a key role in this area. Research has shown that the involvement of women – in different capacities and roles, in both the private and public spheres – is essential to effective prevention efforts. As gatekeepers to their communities, they are often well-positioned to serve as credible, resonant voices against violent radical ideologies. The Office can support local initiatives that engage, inform and empower women to better identify and address violent radicalization in their families and communities. The Office can also develop and share tools, resources and information to support women – and men – in responding to this issue.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

### *Promote Alternative Narratives*

Terrorist groups often aim to influence potential recruits by promoting and spreading certain messages. Promoting positive, alternative narratives is one way to counter such messages.

The Office is looking for ways to support credible voices and empower community actors—particularly youth and women—to develop programs, messaging or other tools that reflect local realities. These measures can be used to challenge violent radical narratives and promote critical thinking. For example, terrorist groups use the Internet and social media to spread violent radical ideologies and messaging quickly and broadly. The Office can support programs that harness these tools for positive uses.

### *Foster Research*

Research is a key element in countering radicalization to violence. It can inform policy development, improve the design of programs and tools, and help identify appropriate and effective ways to counter radicalization to violence. The Government is looking to engage with academics, think tanks and others to determine research priorities, identify best practices and lessons learned and develop effective tools to measure the success of programs.

Through the Kanishka Project<sup>6</sup>, the Government has invested in research about radicalization to violence and has identified a number of best practices. There is more to learn, and the demand for that information and research is great. Support for action-oriented research is important. Such research produces guides, tools and other resources to assist the public, as well as mechanisms to evaluate programs and measure their success. Evaluation tools will help develop more effective programs to counter radicalization to violence. Knowing what works will also inform policies and priorities, and can contribute to the success of Canada's overall approach to the issue.

## **What are other countries doing?**

Countering radicalization to violence is a priority for the international community. The United Nations emphasized the importance of prevention efforts in United Nations Security Council Resolution 2178, which was unanimously adopted in September 2014. Also, in January 2016, the United Nations Secretary-General released a Plan of Action to Prevent Violent Extremism, which encourages countries to develop national strategies for addressing radicalization to violence. Canada strongly supports this initiative.

---

<sup>6</sup> <http://www.publicsafety.gc.ca/cnt/ntnl-scr/cntr-trrrsm/r-nd-flight-182/knshk/index-en.aspx>

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

Like Canada, other countries have begun to develop policies and programs to respond to this issue. Working with communities, engaging youth and women, promoting alternative narratives, and conducting research are also key areas of focus for our international partners.

### *Examples*

Community engagement is a cornerstone of a number of countries' national strategies to counter radicalization to violence. For example, to enhance social cohesion and harmony, Singapore's Community Engagement Programme brings together Singaporeans from different communities – from religious groups, to unions, to educational institutions, to the media – to strengthen inter-communal bonds, build partnerships and enhance social resilience. Also, to better inform citizens on radicalization to violence, Australia has created a website called Living Safe Together as a central online location where people can read about how Australia addresses this issue, seek information and advice on radicalization to violence, and access other resources. The Office could develop similar initiatives that are tailored to the Canadian experience.

Some countries have also explored programs focusing on youth. For example, in Sweden, there is a youth centre called “Fryshust” that promotes confidence, responsibility, and understanding to enable young people to develop their innate abilities and find their way in society. Also, in Denmark, an organization called “My House” aims to pair individuals at risk of radicalization to violence with mentors that face similar challenges and come from similar backgrounds, but that can show an alternative, positive path to explore.

Finally, engaging women in prevention efforts is an important element of some countries' approaches to this issue. For example, in the UK, “Project Shanaz” was developed in 2011 to understand the perception women have of activities related to the country's national strategy to counter radicalization to violence. This project led to the establishment of the Shanaz Network, an independent body of 50 women community leaders that contributes to the development of policies and strategies related to radicalization to violence. A similar model in Canada could help inform the development of a new strategy to counter radicalization to violence.

### **What do you think?**

The Government would like your views about what shape a national strategy to counter radicalization to violence should take. In particular, it is looking to identify policy, research and program priorities for the Office of the community outreach and counter-radicalization coordinator. What should the priorities be for the national strategy?

What should the role of the Government be in efforts to counter radicalization to violence?

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

Research and experience has shown that working with communities is the most effective way to prevent radicalization to violence. How can the Government best work with communities? How can tensions between security concerns and prevention efforts be managed?

Efforts to counter radicalization to violence cannot be “one size fits all.” Different communities have different needs and priorities. How can the Office identify and address these particular needs? What should be the priorities in funding efforts to counter radicalization to violence?

Radicalization to violence is a complex, evolving issue. It is important for research to keep pace. Which areas of research should receive priority? What further research do you think is necessary?

What information and other tools do you need to help you prevent and respond to radicalization to violence in your community?

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## THREAT REDUCTION

Since its creation in 1984, CSIS has collected information and intelligence on threats to the security of Canada, at home and abroad.<sup>7</sup> CSIS uses the information to advise other institutions of government, such as law enforcement, about these threats. These institutions then in turn act on the information.

The ATA, 2015 amended the *Canadian Security Intelligence Service Act (CSIS Act)* to authorize CSIS to reduce threats to the security of Canada. CSIS can now do more than share information. It can also take direct action against threats to reduce the danger they pose. Threat reduction (also called disruption) seeks to prevent or discourage people who pose a threat from carrying out their plans.

The threats facing Canada have evolved significantly in recent years. In part, this flows from the trend away from complex terrorist operations towards loosely organized small-scale attacks, the growing use of the Internet and mobile communications, and the ease with which people can move about the globe. These changes have made it harder for security agencies to prevent attacks.

The RCMP have long had a crime prevention mandate. This allows them to act pre-emptively to prevent threats from materializing. However, there are differences in the roles and responsibilities of CSIS and the RCMP. These include different priorities, different approaches, access to different information and a different international presence. For these reasons, during the development of the ATA, 2015, it was felt that there were situations where CSIS was best placed to take timely action to reduce threats. Even before the debate about the ATA, 2015, a threat reduction mandate for CSIS was being discussed. A 2010 report by SIRC recommended that CSIS seek guidance and direction on the issue of threat reduction. In 2011, the Senate Special Committee on Anti-terrorism also considered threat reduction and issued recommendations.

The CSIS threat reduction mandate does not give it law enforcement powers. For instance, CSIS cannot arrest individuals. CSIS continues to work in consultation with the RCMP and other law enforcement agencies.

### The Threat Reduction Mandate

For some threat reduction measures CSIS requires a warrant from the Federal Court. Whether a warrant is needed hinges on whether the proposed actions by CSIS would affect *Charter* rights or would, without a warrant, be against the law.

---

<sup>7</sup> “Threats to the security of Canada” are defined in section 2 of the *CSIS Act*, and encompass terrorism (or more precisely “acts of serious violence... for the purpose of achieving a political, religious or ideological objective”), espionage and sabotage, foreign-influenced activities that are clandestine, deceptive, or threaten a person, as well as domestic subversion aimed at the overthrow by violence of the constitutional order of government. Lawful advocacy, protest and dissent are excluded, unless carried out in conjunction with any of the activities referred to above.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

*Consider a scenario where a warrant is not needed...*

Mr. C, a Canadian citizen, attends Mr. A's weekly meetings. He has even voiced support for terrorist activity in Canada in response to terrorist propaganda encouraging attacks in the West. Mr. C is seeking employment as a guard for a firm that provides security at major concerts and other events. CSIS approaches the firm and provides information about Mr. C. Once aware of Mr. C's support for terrorist activity, the firm launches an investigation and decides to restrict Mr. C's work. As a result, Mr. C does not gain privileged access to major events where he could pose a security threat.

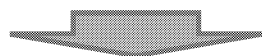
*Consider a scenario where a warrant is needed...*

Mr. D, an associate of Mr. A, is promoting extremism on his personal website by posting videos supporting a terrorist group. His website is hosted outside Canada and also includes how-to guides for making bombs and suicide vests. CSIS obtains a threat reduction warrant from the Federal Court allowing it to modify the website's how-to guides. CSIS replaces some of the terrorism-related details with misinformation that will make the devices fail. Mr. D and his followers do not notice the changes. As a result, their effective support to terrorism has been limited.

The table below sets out the differences between threat reduction measures by CSIS that require a warrant and those that do not.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

	No warrant required	Warrant required
Examples	<ul style="list-style-type: none"> <li>- Interviews</li> <li>- Asking friends to intervene</li> <li>- Reporting extremist content to social media providers</li> </ul>	<ul style="list-style-type: none"> <li>- Disrupting financial transactions</li> <li>- Interfering with terrorist communications</li> <li>- Manipulating goods intended for terrorist use</li> </ul>



Procedure CSIS must follow to take threat reduction measures	<ul style="list-style-type: none"> <li>- CSIS must have reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada</li> <li>- CSIS must demonstrate that the proposed measure is reasonable and proportional in the circumstances</li> <li>- CSIS must obtain internal approval, perform a risk assessment, and consult law enforcement and other agencies as appropriate</li> </ul>	<ul style="list-style-type: none"> <li>- CSIS must have reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada</li> <li>- CSIS must demonstrate that the proposed measure is reasonable and proportional in the circumstances</li> <li>- CSIS must obtain internal approval, perform a risk assessment, and consult law enforcement and other agencies as appropriate</li> <li>- <b>CSIS must obtain approval from the Minister of Public Safety and Emergency Preparedness for a warrant application</b></li> <li>- <b>The Federal Court then reviews the warrant application and decides whether to issue the warrant</b></li> </ul>
--	---	---

Threat reduction measures that would cause death or bodily harm, violate a person's sexual integrity or interfere in the course of justice are prohibited.<sup>8</sup>

<sup>8</sup> See *CSIS Act*, section 12.2.



*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## Potential Impacts on *Charter* Rights

Threat reduction measures may affect Canadians' *Charter* rights and freedoms, depending on the circumstances of the measure.

CSIS must obtain a warrant from the Federal Court before it can take threat reduction measures that would affect rights protected under the *Charter*. The *Charter* recognizes that rights and freedoms are not absolute and that at times they may justifiably be limited. A warrant shows that the Court has determined in advance that the proposed threat reduction measures are reasonable and proportional in the circumstances.

Warrants have long been used to balance government objectives and *Charter* rights. Since 1984, CSIS has sought warrants from the Federal Court to collect intelligence using techniques that limit privacy rights protected by section 8 of the *Charter*. Police wiretaps and search warrants work in a similar way. Threat reduction warrants are a departure from previous warrant regimes. They can limit additional *Charter* rights, not just privacy rights under section 8.

## What are other countries doing?

Intelligence and security services in many of Canada's allies have the mandate to reduce threats to national security and a range of threat reduction powers. There is no standard approach to threat reduction, however, as each country has a unique system of government, making direct comparisons difficult. In some countries, responsibility for national security and intelligence is divided between foreign and domestic services. In others, responsibility is divided between intelligence and law enforcement. In the U.S., for example, there are distinct domestic and international agencies. Domestically, the FBI has both intelligence and law enforcement responsibilities.

Nonetheless, various allied intelligence and security services have the authority to take direct action against threats, domestically and/or abroad, subject to various limitations. In the UK, for instance, the Security Service (also known as MI5) has legal authority to take action to protect national security, including against the threat of terrorism. The Australian Secret Intelligence Service has a broad mandate to undertake "other activities", including threat reduction measures outside of Australia. French authorities can also disrupt threats to France and French interests abroad.

Internationally, the means by which threat reduction activity is legally authorized takes various forms. Canada's framework requires court warrants for measures that would affect *Charter* rights. In other countries, senior members of the executive branch authorize intrusive threat reduction measures.

In the current international environment, the threat reduction mandate allows CSIS to contribute to a broader range of allied operations against terrorism and other shared threats than was previously the case.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## What do you think?

The Government wants to know what you think about CSIS's new threat reduction mandate:

CSIS's threat reduction mandate was the subject of extensive public debate during the passage of Bill C-51, which became the ATA, 2015. Given the nature of the threats facing Canada, what scope should CSIS have to reduce these threats?

Are the safeguards around CSIS's threat reduction powers sufficient to ensure that CSIS uses them responsibly and effectively? If current safeguards are not sufficient, what additional safeguards are needed?

The Government has committed to ensuring that all CSIS activities comply with the *Charter*. Should subsection 12.1(3) of the *CSIS Act*<sup>9</sup> be amended to make it clear that CSIS warrants can never violate the *Charter*? What alternatives might the Government consider?

---

<sup>9</sup> Subsection 12.1(3) of the Act states that CSIS “shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms* or will be contrary to other Canadian law, unless [CSIS] is authorized to take them by a warrant....”

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## DOMESTIC NATIONAL SECURITY INFORMATION SHARING

National security institutions need information to detect, analyze, investigate and prevent threats. It often takes multiple pieces of information to provide a complete threat picture, and today's national security threats can evolve rapidly, heightening the need for timely and complete information.

Yet information needed for national security purposes can be held in different places by various institutions of government. Because of this, the sharing of information is an important part of national security work today. The report of the Air India inquiry<sup>10</sup> stressed this point. The report of the O'Connor inquiry<sup>11</sup> also mentioned the importance of information sharing for investigations and prevention of national security threats, but also highlighted the need for caution with respect to the content of the information and its use by the recipient.

Federal institutions with national security responsibilities can collect information to carry out lawful duties and responsibilities. This collection may be authorized by an Act of Parliament, the common law or the Crown Prerogative. Even institutions that do not have a national security mandate (such as the Department of Fisheries and Oceans) sometimes hold information that could be important for national security institutions. Non-national security institutions must be able to disclose that information to institutions that have a mandate to act on it.

Government institutions must follow certain rules when sharing information, especially information about individuals. These rules are important to protect privacy rights. However, their complexity can sometimes make it difficult to know whether a given institution is permitted to share information. This can prevent information from getting to the right institution in time.

### *The Privacy Act*

The *Privacy Act* protects individuals' personal information by regulating how federal government institutions collect, use, retain and disclose it. The Act limits the collection of personal information by government institutions to that which relates directly to their work. It also limits when this information can be used and disclosed without the consent of the individual to whom it relates.

The *Privacy Act* recognizes that personal information may be disclosed without consent in some situations, including those involving national security. The main exceptions to the rule preventing disclosure without consent are as follows:

1. "Consistent use": One federal institution may share information with another institution for the purpose for which the information was collected or for a use consistent with that purpose (for an example, see the scenario below).
2. "Investigative bodies": Some institutions are listed as "investigative bodies" in the Act (for example, the RCMP and CSIS). An investigative body can ask another federal institution to provide it with personal information to assist it in carrying out its activities. However, the

---

<sup>10</sup> Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

<sup>11</sup> Commission of Inquiry into the Actions of Officials in Relation to Maher Arar.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

other institution must be asked first. It cannot decide on its own to proactively share personal information with an investigative body.

3. “Public interest”: The head of a federal institution may disclose personal information if the head determines that the public interest benefit in disclosure clearly outweighs any invasion of privacy. In the national security context, communicating what the benefit is to a non-national security institution to obtain disclosure may not be possible (for example because of operational sensitivities). This makes it difficult for the head of the non-national security institution to decide whether to disclose personal information in the public interest.
4. “Lawful authority”: the *Privacy Act* permits disclosure of personal information where another Act of Parliament authorizes it.

*Consider a scenario...*

A foreign national, Ms. E, sends an application for permanent resident status to Immigration, Refugees and Citizenship Canada (IRCC). This application contains the personal information that the Government needs to process her request to become a permanent resident and to determine whether she is admissible to Canada under the *Immigration and Refugee Protection Act*. To assess her application for security concerns, IRCC discloses some of Ms. E's personal information to CSIS, which has a security screening mandate under the immigration program. This type of sharing between IRCC and CSIS is an example of sharing that takes place under the “consistent use” exception of the *Privacy Act*.

## **The Security of Canada Information Sharing Act**

### **Objective**

The ATA, 2015 enacted the *Security of Canada Information Sharing Act* (SCISA) to facilitate national security information sharing. The SCISA creates an explicit disclosure authority, which provides greater certainty about when institutions can share information for national security reasons. Because it is an Act of Parliament that authorizes disclosure, it satisfies the “lawful authority” exception under the *Privacy Act*, as explained above.

### **What the SCISA Does**

The SCISA authorizes all federal institutions to disclose information (including information about individuals) related to “activities that undermine the security of Canada.” “Activity that undermines the security of Canada” is defined as any activity that “undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada” (section 2 of the SCISA). This concept covers a broad range of national security-related activities and is intended to provide flexibility to accommodate new forms of threats that may arise. The SCISA includes examples of these activities that may be covered by this concept.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

Information may be disclosed to 17 federal institutions listed in the SCISA (referred to as “recipients” throughout this document).<sup>12</sup> To be disclosed, the information must be *relevant*<sup>13</sup> to the recipient’s lawful national security jurisdiction or responsibilities.

*Consider a scenario...*

During a routine check, a passport official at IRCC contacts the references of Mr. F, who has applied for a passport. Mr. F has been attending Mr. A’s weekly meetings. Without prompting, one referee tells the passport official that she is worried that Mr. F may be travelling to a country to become a fighter with a terrorist group, since he supports the group’s goals. IRCC proactively shares information under the SCISA with CSIS and the RCMP, which have responsibilities for investigating this type of activity.

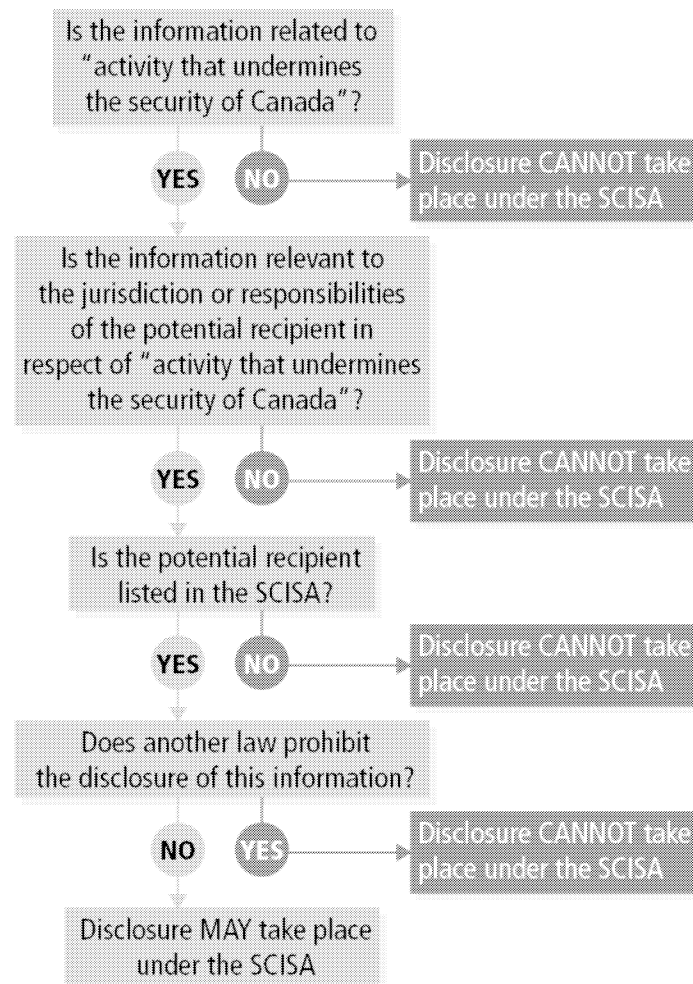
To decide whether they can disclose information under the SCISA, federal institutions go through the following process:

---

<sup>12</sup> These 17 recipients already have legal authorities to collect information for national security reasons. The SCISA neither expands nor changes these collection authorities.

<sup>13</sup> Relevant: Because national security information sharing often engages privacy rights, the SCISA requires that information be disclosed only if it is actually—and not potentially or possibly—relevant to the recipient’s lawful responsibilities for activity that undermines the security of Canada. There must be a reasonable basis to conclude that the information is related to the recipient’s exercise of their responsibilities for such activity. Reliability and accuracy are also important factors in determining whether information is relevant under the SCISA.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*



### When the SCISA Can and Cannot be Used:

The definition of “activity that undermines the security of Canada” only includes activities that have an impact on national security. Some Canadians expressed concern during the parliamentary examination of the bill that became the ATA, 2015 that their right to lawful protest may be impacted by the SCISA. The SCISA was amended to make it clear the activities of advocacy, protest, dissent, and artistic expression *do not* fall within the definition of “activity that undermines the security of Canada.” As a result, information about these activities cannot be disclosed under the SCISA.

However, if violent actions take place that meet the definition of “activity that undermines the security of Canada,” they cannot be considered to be advocacy, protest, dissent or artistic expression. Information about these actions can be disclosed under the SCISA.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

### *Consider another scenario...*

A national park is located near a natural gas pipeline, a critical infrastructure site. An official at the park notices a group gathering to protest near the pipeline. Even though this information deals with critical infrastructure, the official cannot disclose this information under the SCISA to another federal institution. This is because protest, advocacy, dissent, and artistic expression are explicitly excluded from the definition of “activity that undermines the security of Canada” under the SCISA.

### **What the SCISA Does Not Do**

The SCISA cannot be used to bypass other laws prohibiting or limiting disclosure. If another law restricts use or sharing of information, these restrictions continue to apply and must be respected. For example, Employment and Social Development Canada's program legislation addresses how it protects and discloses personal information. The SCISA does not override this program legislation.

### **Who Decides Whether to Use the SCISA?**

The institution disclosing information is responsible for determining whether the information may be disclosed. The disclosing institution may need discussions with the potential recipient to see if the information relates to the national security responsibilities of the recipient. These discussions should not require the sharing sensitive operational information.

An institution has the discretion whether or not to disclose information under the SCISA. This decision always rests with the disclosing institution even if all the SCISA requirements for disclosure are met.

### **Who Receives the Information?**

All recipients under the SCISA have national security responsibilities. However, not necessarily all parts of the recipient institutions will be involved in carrying out these responsibilities. The SCISA requires that information be provided to the head of the institution or to delegates of the head. This helps to ensure that only officials who need the information receive it.<sup>14</sup>

### **Potential Impacts on *Charter* Rights**

The *Charter* protects individuals' privacy against unreasonable government intrusions. The *Charter* allows intrusions into privacy that are authorized by a reasonable law. In some cases, disclosure of information among federal institutions could impact privacy rights.

Information sharing under the SCISA may be reviewed like other instances of government information sharing. In particular, the *Privacy Act* allows the Privacy Commissioner of Canada to review institutions' handling of personal information and to hold institutions accountable by

---

<sup>14</sup> Once information is disclosed to a recipient under the SCISA, the recipient may further disclose it under the SCISA or under another authority outside the SCISA. The recipient's use of the information disclosed to it under the SCISA continues to be governed by authorities found outside the SCISA.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

releasing public reports. Some institutions – the RCMP, CSIS and the CSE – also have specific bodies that review their work, including information sharing practices that are part of this work.

The SCISA includes a power to make regulations; however no regulations have been made. Regulations made under the SCISA would support how the SCISA works in practice. For example, regulations could outline record-keeping requirements.

A number of government-wide information sharing guidance and support resources are available for federal institutions. Public Safety Canada has prepared a deskbook and a public framework to guide institutions in using the SCISA. Federal institutions may also set policies and give guidance on how their officials should use the SCISA.

## What are other countries doing?

Many countries seek to promote the sharing of information for national security purposes, while protecting the privacy rights of individuals. As each country has a unique legislative and policy framework for the sharing of information for national security purposes, the challenges they face in this area vary considerably across jurisdictions. Some countries allow the sharing of information between government agencies without express consent to do so in each case. Others have more explicit powers or policies.

The UK's information sharing provisions are included in its *Counter-Terrorism Act, 2008*. These provide broad information sharing powers, including from persons to UK security agencies. Denmark has express authority in privacy legislation (the *Act on Processing of Personal Data*) to share personal information for national security purposes. Australia has a 10-year plan (Vision 2020) to enhance national security information sharing, which includes a harmonized policy and legislative framework.

## What do you think?

The Government has made a commitment to ensure that Canadians are not limited from lawful protest and advocacy. The SCISA explicitly states that the activities of advocacy, protest, dissent, and artistic expression do not fall within the definition of “activity that undermines the security of Canada.” Should this be further clarified?

Should the Government further clarify in the SCISA that institutions receiving information must use that information only as the lawful authorities that apply to them allow?

Do existing review mechanisms, such as the authority of the Privacy Commissioner to conduct reviews, provide sufficient accountability for the SCISA? If not, what would you propose?

To facilitate review, for example, by the Privacy Commissioner, of how SCISA is being used, should the Government introduce regulations requiring institutions to keep a record of disclosures under the SCISA?

Some individuals have questioned why some institutions are listed as potential recipients when their core duties do not relate to national security. This is because only part of their jurisdiction or



*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

responsibilities relate to national security. Should the SCISA be clearer about the requirements for listing potential recipients? Should the list of eligible recipients be reduced or expanded?

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## THE PASSENGER PROTECT PROGRAM

Air travel is an important means of transportation, both within Canada and abroad. Without appropriate security measures, air travel is vulnerable to criminal and national security threats. Tragedies such as the 1985 Air India bombing, the attacks of September 11, 2001, and the October 2015 bombing of a Russian airliner in Egypt, each demonstrate the cost in lives, economic and social disruption that threats to aviation security can cause.

Direct threats to aviation security, such as terrorists bringing or placing explosive devices aboard aircraft, continue to be of concern. In addition, concern is growing about individuals travelling abroad, often by air, to engage in terrorism offences. These individuals are known as “extremist travellers.” They pose a threat at home and also pose a threat abroad when they participate in conflicts in countries as Syria and Iraq. These individuals are involved in training, fundraising and other terrorist activities on behalf of groups such as Daesh. Trained, radicalized and experienced extremist travellers pose another serious risk if they return to Canada. Here, they might launch or inspire domestic attacks.

The Government provides aviation security in part by preventing individuals who have the intent and capability to harm passengers and aircraft from boarding. The ATA, 2015 enacted the *Secure Air Travel Act* (SATA). Under the SATA, the Government can use the Passenger Protect Program (PPP) – an air passenger identity screening program – to prevent individuals from boarding a flight if they pose a threat to transportation security or are seeking to travel by air to commit certain terrorism offences.

### *Consider a scenario...*

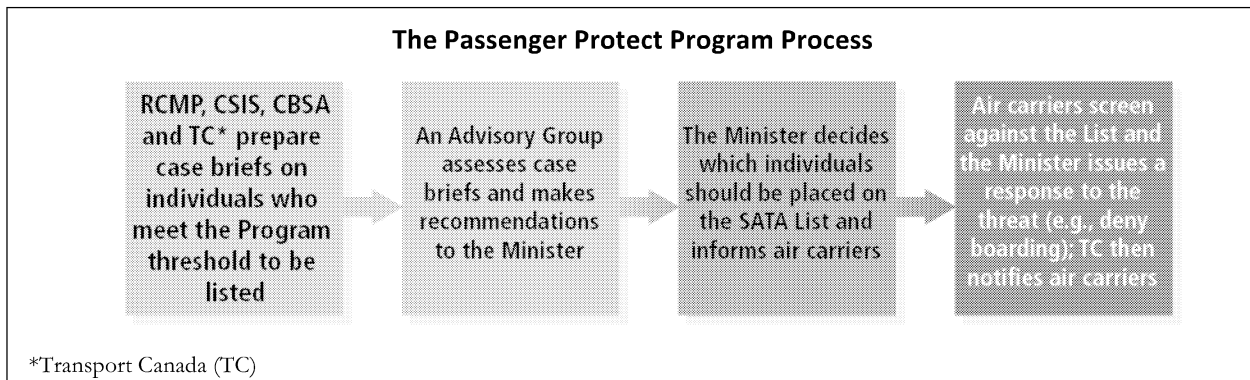
Ms. G is a 22-year-old high school graduate who has been drifting between jobs over the past few years. She attends Mr. A's discussion meetings in her neighbourhood and has rapidly radicalized to violence.

Ms. G is keen to travel overseas to join a terrorist group. Mr. A has been communicating with a terrorist overseas to plan Ms. G's departure. The goal is for Ms. G to get weapons and explosives training and fight for her cause. She then wants to return to Canada and train others to become terrorists.

The RCMP become aware of Ms. G's plans and alert Public Safety Canada. Based on this information, the Minister of Public Safety and Emergency Preparedness adds Ms. G to the list created under the SATA. If Ms. G attempts to check in for a flight, Public Safety Canada will be alerted and may issue a direction to deny her boarding.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

The PPP, as governed by the SATA, works as follows:



Through the PPP, the Minister of Public Safety and Emergency Preparedness (the Minister<sup>15</sup>) has the authority to establish a list of individuals (known as the SATA List) who may (1) pose a threat to transportation security or (2) travel by air to commit certain terrorism offences.<sup>16</sup> Listed individuals can be prevented from flying. To list an individual, the Minister must have reasonable grounds to suspect that the individual will engage in at least one of these two acts. For example, if it is reasonably suspected that an individual will travel by air to commit certain terrorism offences,<sup>17</sup> such as to participate in the activities of a terrorist group, the individual can be listed under the PPP.

The listing process is conducted confidentially and is based on intelligence and other information from investigations. Public Safety Canada chairs an advisory group composed of the RCMP, CSIS, the CBSA, TC and IRCC. The advisory group nominates individuals to the SATA List, assesses the information supporting the nominations and recommends to the Minister which individuals should be listed. The SATA List is reviewed at least every 90 days to ensure that there are still reasonable grounds to suspect that individuals on the List pose a threat to transportation security and/or will travel by air to commit certain terrorism offences.

Once an individual is listed, the Minister can direct an air carrier on how to respond when the individual attempts to board an aircraft. The direction will be issued to air carriers only once an individual's identity is verified and confirmed to be a positive match to the SATA List, and after any new information is considered. These responses are tailored to the specific situation, based on what is reasonable and necessary to prevent the threat from being carried out. For example, individuals who are assessed as posing a high risk to transportation security may be denied boarding to protect both passengers and aircraft. Other listed individuals may undergo additional screening to provide greater certainty that they are not, for example, carrying any weapons or prohibited items.

<sup>15</sup> The Minister can delegate his or her authority to take any action under the SATA.

<sup>16</sup> Pursuant to paragraphs 8(1)(a) and (b) of the SATA.

<sup>17</sup> The SATA refers to offences under sections 83.18, 83.19 and 83.2 of the *Criminal Code*.

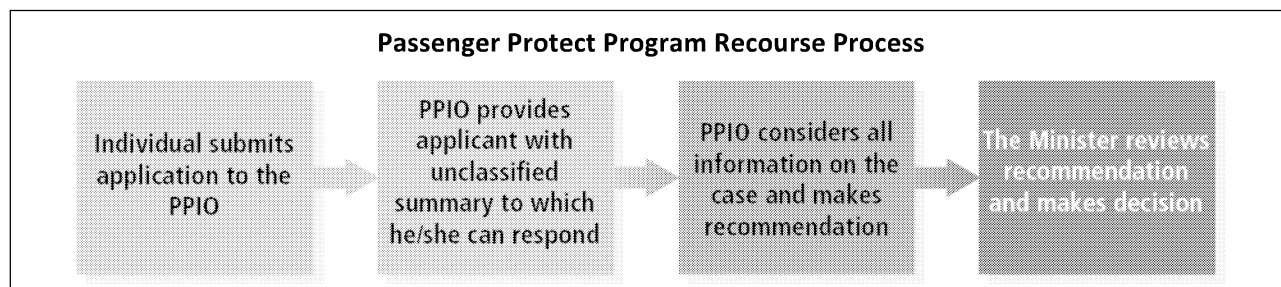
*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## Potential Impacts on *Charter* Rights

A direction to deny boarding can impact a citizen's right to enter and leave Canada. Section 6 of the *Charter* protects this right. Individuals also have an interest in not being delayed or prevented from travelling by air. A direction to deny boarding would only be made when the Minister considers it is reasonable and necessary to prevent a listed person from taking a specific action.

### Recourse

Because of the acknowledged impacts of being denied boarding, an individual in this situation can apply in writing for recourse to the Passenger Protect Inquiries Office (PPIO) within 60 days of being denied boarding.<sup>18</sup> The application seeks to have the individual's name removed from the List. The applicant receives an unclassified summary of the information used to support the listing and has an opportunity to respond. The Minister may take up to 90 days<sup>19</sup> to review the application and decide whether there are still reasonable grounds to maintain the applicant on the List. If the Minister does not make a decision within 90 days,<sup>20</sup> the Minister is deemed to have decided not to remove the applicant's name from the List. This is done to err on the side of caution, while the 90-day deadline ensures that the applicant has timely access to the Federal Court, as explained below.



If an individual is not satisfied with the Minister's decision, the individual may appeal the decision to the Federal Court. Most decisions made under the PPP rely on sensitive information that, if disclosed, could be injurious to national security or endanger the safety of a person. The judge hearing the appeal can see all information relevant to the Government's decision. To protect against disclosure of sensitive information, the applicant sees a summary of the relevant sensitive information. The applicant can also introduce new information to respond to the Government's case. The judge may appoint an *amicus curiae* to assist the Court with any aspect of the proceeding, including during the closed portion of the proceedings where the applicant cannot be present because sensitive information is being presented.

<sup>18</sup> Subsection 15(2) of the SATA allows the Minister to extend that limit if there are exceptional circumstances.

<sup>19</sup> Subsection 15(6) of the SATA allows this period to be extended, as agreed by the applicant and the Minister.

<sup>20</sup> Or a further period agreed upon between the applicant and the Minister.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

### *Consider a scenario...*

Mr. H intends to fly to Florida for the Labour Day weekend but is delayed at the airline ticket counter while the desk agent contacts his supervisor. After a few minutes, Mr. H is allowed to continue, but he leaves on his flight frustrated. He suspects that his name is similar to that of someone on Canada's aviation security list. He contacts the Passenger Protect Inquiries Office, which works with relevant partners to help facilitate his future travel.

### **Redress**

The SATA List is not the only reason for delaying an individual or preventing them from flying. There can be many other reasons, unrelated to the SATA, including air carriers' own security lists and/or aviation security lists maintained by other countries. As well, a false positive match to an aviation security list, whether that of an air carrier, a foreign country or the SATA List itself, may cause travel to be delayed.

The PPIO provides assistance to air travellers who have experienced delays or difficulties related to aviation security lists. The PPIO can assist the traveller in identifying the reason for this situation and suggest what to do next. Following a joint announcement by the Prime Minister of Canada and the President of the United States on March 10, 2016, the governments established the Canada-U.S. Redress Working Group. The Working Group is a bilateral mechanism. It allows the PPIO to collaborate closely with the U.S. on certain matters of redress and recourse about Canadian and American citizens and permanent residents who may be affected because of their potential presence on the SATA List or the U.S. No Fly List.

In addition, the Government is considering possible changes to the SATA and its regulations to help reduce instances of false positive matches to the SATA List. The objective is to create a process where individuals who have experienced a false positive match can obtain a redress number, which would be provided to the air carrier prior to travel and assist in avoiding delays.

### **What are other countries doing?**

A number of Canada's key international partners, including the U.S., the UK, Australia and New Zealand have some form of air passenger screening prior to departure. In most cases, these programs are designed to determine an individual's admissibility status before they can travel to that country, and/or whether they pose a security risk. The U.S., for example, operates a number of air passenger screening programs that address both immigration and security considerations.

Canada's PPP does not operate in conjunction with the U.S. No Fly list or with any other countries' and organizations' aviation security programs. While the SATA permits the Minister of Public Safety to share information with another country to address potential threats, both countries' programs will continue to operate subject to their respective laws.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## **What do you think?**

At present, if the Minister does not make a decision within 90 days about an individual's application for removal from the SATA List, the individual's name remains on the List. Should this be changed, so that if the Minister does not decide within 90 days, the individual's name would be removed from the List?

To reduce false positive matches to the SATA List, and air travel delays and denials that may follow, the Government has made a commitment to enhance the redress process related to the PPP. How might the Government help resolve problems faced by air travellers whose names nonetheless generate a false positive?

Are there any additional measures that could enhance procedural fairness in appeals of listing decisions after an individual has been denied boarding?

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## CRIMINAL CODE TERRORISM MEASURES

The *Criminal Code* defines terms such as “terrorist activity,” “terrorism offence” and “terrorist group.” It sets out a wide range of terrorism offences, provides a process to “list” entities as terrorist groups and outlines a range of anti-terrorism powers for law enforcement.<sup>21</sup> Many of the terrorism provisions were enacted in 2001 and amended in 2013 to include specific terrorist travel offences. Since 2001, a number of people have been convicted of terrorism offences in Canada, with some receiving life sentences. The courts have found key *Criminal Code* terrorism provisions to be consistent with the *Charter*.<sup>22</sup>

Some provisions of the ATA, 2015 introduced changes to *Criminal Code* terrorism provisions. The Code was amended to accomplish several goals:

- to make it easier for peace officers to detain individuals temporarily, and to apply to a court to have reasonable conditions imposed on individuals to prevent the carrying out of terrorist activity and the commission of terrorism offences;
- to create a new offence that criminalizes the advocacy or promotion of the commission of terrorism offences in general;
- to give the courts the authority to order the seizure and forfeiture of tangible terrorist propaganda material and the removal of online terrorist propaganda from Canadian websites; and,
- to provide additional protection to witnesses and other participants in national security proceedings and prosecutions.

### Preventive Law Enforcement Tools (Recognizance with Conditions and Terrorism Peace Bond)

Canadian criminal law generally focuses on prosecuting offences that have already occurred. However, criminal courts can also impose **preventive conditions** on an individual where there is evidence that the individual is likely to commit an offence in future. Two specific tools allow for a court to impose conditions to prevent terrorism: the **recognizance with conditions** and the **terrorism peace bond**. Some aspects of these tools first appeared in 2001 when the *Anti-terrorism Act* came into force.

---

<sup>21</sup> “Terrorist activity” is a term made up of a list of specific offences that implement Canada’s international obligations, as well as a general definition. It is used as the basis for many of the terrorism offences in the *Criminal Code*, such as knowingly facilitating a terrorist activity

<sup>22</sup> See, for example, *R. v. Khawaja* [2012] 3 SCR 555.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

A **terrorism peace bond** is used to prevent a specific individual from committing a terrorism offence, such as leaving or attempting to leave Canada to commit an offence for a terrorist group.

A **recognizance with conditions** is used when the police suspect someone is connected in some way to the carrying out of a terrorist activity. For example, they suspect that someone is connected to a broad plot to attack Parliament, but the person's exact role may not be known.

Both the terrorism peace bond and the recognizance with conditions aim to prevent individuals from carrying out terrorist acts.

*Consider a scenario where a terrorism peace bond could be used...*

A family notifies the RCMP that they feel their son, Mr. I, has become radicalized to violence. He is a good friend of Mr. A. The RCMP investigate and learn that Mr. I has told a number of people close to him that he plans to join a terrorist group active in a conflict zone abroad. The RCMP also learn that Mr. I has been pricing air travel to a country that borders an ongoing conflict zone where the group is active.

The RCMP now suspect that Mr. I may commit a terrorism offence – travelling or attempting to travel abroad to participate in the activity of a terrorist group. They seek the consent of the Attorney General of Canada to apply to a judge for a terrorism peace bond to prevent Mr. I from travelling abroad.



*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

*Consider a scenario where a recognizance with conditions could be used...*

The police conduct an urgent investigation into a group of ten people based on an anonymous tip. Some of these people attend Mr. A's weekly meetings. Some members of the group are apparently planning to bomb an unknown public gathering that week. Further investigation reveals that one person in the group, Ms. J, recently downloaded bomb-making instructions. The police hope to obtain a recognizance with conditions to stop Ms. J from making, providing or using an explosive device. They seek the consent of the Attorney General of Canada to apply to a judge for a recognizance with conditions.

The judge considers the application and is satisfied that a terrorist activity may be carried out. The judge also has reasonable grounds to suspect that the imposition of the recognizance with conditions is likely to prevent the carrying out of the terrorist activity. As a result, the judge issues a recognizance with conditions.

The ATA, 2015 amended the provisions on recognizance with conditions and the terrorism peace bond. The amendments were designed to make it easier for police to apply to provincial court for the imposition of reasonable conditions, such as travel restrictions.

The 2015 amendments did the following:

- lowered the threshold to obtain a **recognizance with conditions** to where a peace officer believes on reasonable grounds that a terrorist activity “may be carried out.” Previously, the law required that police believe on reasonable grounds that a terrorist activity “will be carried out.” The amendments also replaced the former requirement that a recognizance is “necessary to prevent” the carrying out of a terrorist activity with “is likely to prevent.”
- increased the period of detention before a recognizance with conditions hearing is held to up to seven days, which includes periodic review by a judge. Previously, such detention could last only up to three days – a possible 24-hour police-initiated detention and a 48-hour judge-ordered detention.

Further periods of detention beyond the possible 24-hour initial police detention are allowed only if the judge finds that it is necessary to ensure public safety, to ensure that the person attends the hearing or to maintain confidence in the administration of justice. In addition, there are two new possible 48-hour periods of judge-ordered detention. In these instances, it must also be demonstrated that the investigation in relation to which the person is being detained is being conducted “diligently and expeditiously.” If these criteria are not met, the person must be released – with or without conditions – but will be required to return to court for the hearing on whether conditions should be imposed on them.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

- lowered the threshold to obtain a **terrorism peace bond** so that it may be obtained when a person believes an individual “may commit” a terrorism offence. Previously, the threshold was “will commit” a terrorism offence.
- for both the recognizance with conditions and the terrorism peace bond, there are now additional requirements for the judge to consider whether to impose a geographical restrictions condition on the person and whether to require the person to surrender their passport(s) or other travel documents.
- increased the length of time these measures can be applied if the person has been previously convicted of a terrorism offence. For the recognizance with conditions, the conditions can apply for up to two years. For the terrorism peace bond, the conditions can apply for up to five years.
- if a person breached their conditions under a recognizance with conditions or a terrorism peace bond, increased the maximum penalty to four years imprisonment (from a maximum of two years).
- sought to improve the efficiency and effectiveness of the recognizance with conditions and peace bonds across Canada by allowing for the use of video conferencing and for the transfer of peace bonds between provinces.

### Potential Impacts on Charter Rights

The terrorism peace bonds and recognizance with conditions impact liberty interests protected under the *Charter*. Persons subject to these measures may face detention and other restrictions on their liberty without being charged with or convicted of an offence.

The consent of the Attorney General of Canada or of a province is required before the police can even apply to a judge for a recognizance with conditions or terrorism peace bond. In addition, the Crown or the affected person may apply to change any of the conditions. The recognizance with conditions also continues to be subject to a requirement to report annually on its use, whereas no similar reporting requirement applies in respect of the terrorism peace bond. Finally, the provisions on these recognizances are subject to a five-year sunset clause. This means that the recognizance provisions will no longer be in force five years after July 15, 2013, unless Parliament renews them.

### Criminalizing the Advocacy or Promotion of Terrorism Offences in General

The ATA, 2015 added a new *Criminal Code* offence on advocating or promoting the commission of terrorism offences in general.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

*Consider a scenario...*

Ms. K has also been attending Mr. A's weekly discussion groups. She feels that what Mr. A is saying should be known by more people and that Mr. A's views deserve a wider audience. To do this, Ms. K has started posting some of her views online. Over time, she has gained some followers on social media. She is now clearly stating that violence should be used as the only way to change the Government's position on foreign policy.

Ms. K has been communicating with some of her online followers. One has stated that they would be willing to "take direct action." In response to what she believes is support for her views, she decides to use her latest post to appear in a video message dressed in military clothing. In the video, she urges her followers to support a terrorist group by saying, "Do not wait for us to tell you what to do. From now on, you have permission to do whatever you want, do whatever is in your capability. Just act."

As noted above, the 2015 change to the *Criminal Code* makes it a criminal offence for a person, by communicating statements, to knowingly advocate or promote the commission of terrorism offences in general. To commit the offence, the person must *know* that any of those offences will be committed or *be reckless* as to whether any of those offences may be committed as a result of such communication.

Counselling generally involves one person procuring, soliciting or inciting another to commit a criminal offence. Counselling is a long-standing offence. It requires some specificity about the offence or type of offence being counselled.

The definition of "terrorism offence" in the *Criminal Code* includes a broad range of conduct – from violence against people and destruction of property to providing financial and material support and recruitment. Before the 2015 change to the *Criminal Code*, the scope of the offence of counselling was unclear. There was some uncertainty about whether it constituted counselling if a person actively encouraged committing terrorism offences but was not specific about the offences or the type of offences (for example, whether terrorist bombing or terrorist financing). There was also uncertainty about what the penalty would be. This new offence makes it clear that such conduct is criminal. The new offence is modelled on the existing law of counselling. It extends the concept of counselling to cases where no specific terrorism offence is being counselled, but where it is evident nonetheless that terrorism offences are being counselled.

The maximum penalty for the new offence is five years imprisonment. This is the same maximum as that for advocating or promoting genocide against an identifiable group, the most serious of the three hate propaganda offences in the *Criminal Code*.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## Potential Impacts on Charter Rights

Because this offence criminalizes communicating statements, it could be viewed as limiting freedom of expression. However, it is important to consider that the expression in question is generally directed at violent activities. As well, this offence involves more than mere expression. The offence is not an attempt to criminalize glorification of terrorism or praise of terrorism. The offence prohibits active encouragement to commit terrorism offences, not mere expressions of opinion about the acceptability of terrorism.

To ensure appropriate oversight, the prior consent of the appropriate Attorney General is needed to begin proceedings in respect of terrorism offences.

## Seizure and Forfeiture (or Removal) of Terrorist Propaganda

The ATA, 2015 created two new warrants of seizure (court orders that allow police to seize materials) in the *Criminal Code* to apply to “terrorist propaganda” material. This is material counselling the commission of a terrorism offence or advocating or promoting the commission of terrorism offences in general.

Related amendments to the *Customs Tariff* also allow CBSA border services officers to seize terrorist propaganda being imported into Canada without a warrant, as they would other contraband.

Some Canadians raised concerns about the definition of terrorist propaganda during the debate about the ATA, 2015. The Government has made a commitment to address the issue.

The new provisions allow a judge to order the seizure and forfeiture of terrorist propaganda material that is in printed form or is in the form of audio recordings. A judge may also order the removal of terrorist propaganda when it is in electronic form and is made available to the public through a Canadian Internet service provider (ISP).

*Continuing the scenario from above...*

Ms. K's posts on social media are made available through a Canadian ISP. Her posts have clearly been promoting the commission of terrorism offences in general.

With the consent of the Attorney General, the police seek a warrant from a judge requiring the Canadian ISP to remove this content from the site.

## Potential Impacts on Charter Rights

The new warrants could impact the right to free expression. However, the warrants are similar to those already available under the *Criminal Code* for the seizure of material deemed criminal, such as hate propaganda. As well, the consent of the Attorney General is needed before the police can apply for a warrant, to ensure that the Attorney General considers public interest issues, such as protecting freedom of expression.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## Protections for Witnesses and Other Justice System Participants

The ATA, 2015 introduced changes to the *Criminal Code* to improve protection of witnesses, in particular in proceedings involving security information or criminal intelligence information. Security certificate proceedings under the *Immigration and Refugee Protection Act* are examples.

The changes on how witnesses can testify include the following:

- Judges can order that witnesses testify behind a device, such as a screen, to prevent the public from seeing them while they testify;
- Judges must consider whether a witness has responsibilities relating to national security or criminal intelligence when deciding whether to allow that witness to testify using a pseudonym or via closed-circuit television; and
- Judges have explicit authority to make any order necessary to protect the security of any witness, including those who have responsibilities relating to national security. One such order could be to allow a witness to testify while partially disguised.

In addition, the ATA, 2015 amended the *Criminal Code* to better protect justice system participants from intimidation. The *Criminal Code* prohibits their intimidation and provides a maximum of 14 years imprisonment for the offence. The ATA, 2015 amended the *Criminal Code* to expand the definition of “justice system participant” to include persons who play a role in proceedings that involve various types of information, including security information and criminal intelligence information. This ensures that punishment for intimidation is proportional to the gravity of the conduct, its effect on the victims and, more broadly, its effect on the proper functioning of the justice system.

The ATA, 2015 also amended the *Criminal Code* to remove the requirement to publish the names of federally-designated prosecutors and peace officers who have obtained authorizations to intercept private communications (“wiretap” authorizations). This increases protection from intimidation or retaliation for federal prosecutors and law enforcement officers who obtain such authorizations. The amendment puts them in the same situation as their provincial counterparts. The Minister of Public Safety and Emergency Preparedness will continue to report annually to Parliament on the number of federally-designated prosecutors and peace officers who have obtained authorizations for wiretaps. This maintains ministerial accountability for their use.

## Potential Impacts on Charter Rights

These measures on how witnesses can testify could impact the open court principle (the principle that information before a court ought to be public information as far as is possible), which is protected by the *Charter*, because the public is deprived of some information about the proceeding.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

These measures could also impact fair trial rights because some witnesses may testify behind a device shielding their identity.

## What are other countries doing?

### *Terrorism Peace Bonds and Recognizance with Conditions*

The recognizance with conditions and peace bond provisions are consistent with counter-terrorism laws in countries such as the UK and Australia.

The UK, for example, currently allows for pre-charge detention in respect of a terrorist offence for up to 14 days, which also requires independent review on grounds similar to those contained in the ATA, 2015. They also have a tool similar to a peace bond, called a Terrorism Prevention and Investigation Measure, which allows for the imposition of conditions on individuals where satisfied, on the balance of probabilities, that the individual is or has been involved in terrorism-related activity.

Australia also allows for preventative detention which, under federal law, can last for three days. Australian law also permits the imposition of “Control Orders,” which are similar to peace bonds and which can result in the imposition of conditions on individuals where evidence establishes that, for example, making the order would substantially assist in preventing a terrorist act.

### *Advocacy or Promotion of Terrorism Offences in General*

Since 2006, the UK has had an offence of direct or indirect encouragement to commit acts of terrorism. For the purposes of the offence, it is irrelevant whether the encouragement relates to one or more particular acts of terrorism or acts of terrorism generally. Indirect encouragement is defined to include a statement which glorifies the commission of such acts and which members of the public could reasonably be expected to infer that what is being glorified is being glorified as conduct that should be emulated by them in existing circumstances.

In 2014, Australia created a new offence of advocating the doing of a terrorist act or the commission of a terrorism offence, while being reckless as to whether another person will engage in a terrorist act or commit a terrorism offence. “Advocates” is defined to include promoting. It applies where one terrorism act or offence is being advocated or more than one of such acts or offences are being advocated. There are statutory defences that may apply depending on the circumstances, such as publishing in good faith a report or commentary about a matter of public interest. The maximum punishment is five years imprisonment.

As the Canadian offence in ATA, 2015 is based on the knowing and active encouragement of the commission of terrorism offences in general, it more closely resembles the Australian rather than the UK model.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

### *Seizing Terrorist Propaganda*

The measures are similar to laws that already exist in the UK and Australia. For example, the UK legislation, which allows for the takedown of websites and social media feeds, has been in existence since 2006. In Australia, complaints about on-line content are made to the Australian Communications and Media Authority (ACMA). If the ACMA determines that the content is restricted (i.e., if it incites violence or advocates a terrorist act), it issues a notice and takedown order to the service provider.

### *Protecting those Involved in National Security Proceedings/Prosecutions*

The UK, New Zealand, and Australia have all developed legislative regimes that provide ways for witnesses to testify which seek to mitigate any adverse consequences that may arise from their giving testimony, while protecting the interests of an accused.

## **What do you think?**

Are the thresholds for obtaining the recognizance with conditions and terrorism peace bond appropriate?

Advocating and promoting the commission of terrorism offences in general is a variation of the existing offence of counselling. Would it be useful to clarify the advocacy offence so that it more clearly resembles counselling?

Should the part of the definition of terrorist propaganda referring to the advocacy or promotion of terrorism offences in general be removed from the definition?

What other changes, if any, should be made to the protections that witnesses and other participants in the justice system received under the ATA, 2015?

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## PROCEDURES FOR LISTING TERRORIST ENTITIES

Listing an individual or group as a “terrorist entity” is a public means of identifying their involvement with terrorism and curtailing support for them. Listing is one component of the international and domestic response to terrorism.

There are three listing mechanisms in Canada. Two are established under Canada's *United Nations Act*<sup>23</sup> and a third was created by an amendment to the *Criminal Code* in 2001. Domestically, Canada relies mainly on the *Criminal Code* process. The *Criminal Code* process both helps to fulfill Canada's international obligations and supports domestic counter-terrorism measures. An entity listed under the *Criminal Code* fall under the *Criminal Code*'s definition of a terrorist group. Any funds the group has in Canada are immediately frozen and may be seized by, and forfeited to, government.

More than 50 terrorist entities are now listed under the *Criminal Code*. These include al-Qaida and Daesh. To date, most listed entities are based overseas, though members or supporters can also be found in Canada. Entities originating in Canada can also be listed.

The *Criminal Code* listing process begins with the RCMP or CSIS producing criminal or security intelligence reports on an entity. The Minister of Public Safety and Emergency Preparedness may recommend to the federal Cabinet that an entity be listed if the Minister has reasonable grounds to believe that the entity:

- knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity;  
or
- is knowingly acting on behalf of, at the direction of, or in association with an entity that has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity.

To list an entity, Cabinet must also be satisfied that the above test is met. The name of the listed entity is then published in the *Canada Gazette*. A complete list is available on Public Safety Canada's website.

### *Consider a scenario...*

The 123 Group has committed terrorist attacks overseas and is being investigated by CSIS. CSIS informs Public Safety Canada about 123 Group's involvement in these attacks and its links to Canada. The Minister of Public Safety and Emergency Preparedness recommends to Cabinet adding the 123 Group to the list of terrorist entities established under the *Criminal Code* because the group has knowingly carried out a terrorist activity. Cabinet approves the listing. All financial assets

<sup>23</sup> These are the *UN Al-Qaida and Taliban Regulations* and the *Regulations Implementing the UN Resolutions on the Suppression of Terrorism*.



*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

belonging to 123 Group in Canada are frozen and can be seized by government.

The entity and the public are not made aware that the Government is planning to list the entity until the listing takes effect. This is to prevent the entity removing its Canadian assets from Canada before the listing freezes them.

Once an entity is listed, the *Criminal Code* deems it a “terrorist group” in Canada. This can help with investigating and prosecuting terrorism offences since it is not necessary for investigators and prosecutors to prove independently that the individual or group is a terrorist group. It is not a crime simply to be a terrorist group, but many *Criminal Code* terrorism offences contain the term “terrorist group” in the description of the offence. For example, it is an offence to do any of the following:

- knowingly participate in, or contribute to any activity of, a terrorist group for the purpose of enhancing the ability of any terrorist group to facilitate or carry out terrorist activity;
- leave Canada to participate in the activities of a terrorist group;
- collect money or property knowing that it will benefit a terrorist group; and,
- instruct anyone to carry out an activity for the benefit of a terrorist group.

The listing process also makes it easier to apply other provisions relating to terrorist groups, such as using the *Charities Registration (Security Information) Act* to de-register a charity or refuse to register an organization as a charity.

Canada's closest allies, including the U.S., UK, Australia and New Zealand, have similar terrorist listing regimes that include mechanisms for freezing assets in compliance with international obligations.

## Potential Impacts on *Charter* Rights

Being listed as a terrorist entity or being associated with a terrorist entity could impact *Charter* rights. Specifically, section 7 of the *Charter* protects against the deprivation of life, liberty and security of the person, except in accordance with the principles of fundamental justice.

Procedural safeguards have been put in place because of the possible impact of a *Criminal Code* listing on these rights. An entity has the right to apply to the Minister of Public Safety and Emergency Preparedness to be de-listed. If the Minister decides not to de-list the entity, the entity can ask the Federal Court for judicial review of the Minister's decision.

Some of the evidence relating to the listing will be sensitive, and the Government may wish to protect it from being disclosed to the entity. However, this evidence can only be withheld from the entity if a Federal Court judge determines that its disclosure would injure national security or endanger the safety of any person. If evidence is withheld on these grounds, the judge must provide

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

an unclassified summary to ensure that the entity can understand the basis of the listing decision. As part of this process, the entity can also make submissions to the Federal Court. If the judge determines that the listing is unreasonable, he or she will order the entity to be de-listed.

The Government is also required to review all entities on the list every two years and confirm whether they should remain on the list.

Listing an entity could harm individuals and groups with a similar name. To prevent harm from mistaken identity, individuals and groups may apply to the Minister of Public Safety and Emergency Preparedness for a certificate confirming that they are not the entity on the list.

### What are other countries doing?

Canada's closest allies all have similar terrorist listing regimes that include mechanisms for freezing assets in compliance with international obligations. UN Security Council (UNSC) Resolution 1267 and its successor Resolutions, including UNSC Resolution 2253, require states to freeze the assets of the Taliban, Usama bin Laden and his associates, members of Al-Qaida, and members of Daesh. The Resolution also imposes a travel ban and arms embargo against those listed by the UN. Canada implements UNSC Resolution 1267 through the *UN Al-Qaida and Taliban Regulations* and through the *Immigration and Refugee Protection Act*. UNSC Resolution 1373 requires states to freeze without delay, the financial assets of persons and entities engaged in terrorism. This obligation is primarily met in Canada by the list under the *Criminal Code*, but is also implemented through the *Regulations Implementing the UN Resolution on the Suppression of Terrorism*. The manner in which these international obligations are domestically implemented by Canada's allies has led to a variety of different terrorist listing regimes.

The UK, for example, implements its international obligations in relation to UNSC Resolution 1267 using regulations made pursuant to the *European Communities Act 1972*. UNSC Resolution 1373 is implemented under Part 1 of the *Terrorist Asset-Freezing etc. Act 2010*. As well, under the UK's *Terrorism Act 2000*, the Home Secretary may proscribe an organization if it commits or participates in acts of terrorism, prepares for terrorism, promotes or encourages terrorism or is otherwise concerned with terrorism. Membership in a proscribed organization is a criminal offence. Proscribed entities may apply to the Home Office to be de-listed and, if denied, an appeal process to a special commission, as well as judicial review of its decision, is available.

Australia, like Canada, has a listing process in its *Criminal Code*. The government may list an entity if the Attorney-General is satisfied on reasonable grounds that it is directly or indirectly engaged in preparing, planning, assisting or fostering the doing of a terrorist act, or advocates the doing of a terrorist act. The Australian government reviews listed entities every three years from the date that they were originally listed. Any person or organisation is entitled to make a de-listing application to the Attorney-General and judicial review of the legality of a decision to list an organisation is also available in the courts. Australia also implements UNSC Resolution 1373 by regulations made under

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

the *Charter of the United Nations Act 1945*, and implements UNSC Resolution 1267 by automatically incorporating the United Nations sanctions list by regulations made under the same Act.

New Zealand's *Terrorism Suppression Act 2002* provides for a list of terrorist entities to be established and maintained. The police are responsible for coordinating requests to the Prime Minister for designation of a terrorist entity. A designation in New Zealand, like in Canada, has the effect of freezing the entity's assets. It is also a criminal offence to participate in or support the activities of the designated terrorist entity. This includes dealing with the property of the designated terrorist entity or making property or financial services available to the entity. Also, New Zealand implements the UNSC Resolution 1267 and automatically incorporates the United Nations sanctions list by regulations made under their *United Nations Act 1946*.

The lists kept by the U.S. government are more complex and diverse. The U.S. implements its obligations relating to financial sanctions under both UNSCR 1267 and UNSCR 1373 primarily through Executive Order (E.O.) 13224. The Office of Foreign Assets Control administers and enforces E.O. 13224 and maintains a public list of groups and individuals designated under the Order as well as those designated under the *Immigration and Nationality Act* as Foreign Terrorist Organizations. There are some general similarities with Canada's listing processes. For example, entities are not informed that they may be listed and they cannot provide evidence or submissions before the listing process is completed.

## What do you think?

The Government is interested in your views about the listing of terrorist entities.

Does listing meet our domestic needs and international obligations?

The *Criminal Code* allows the Government to list groups and individuals in Canada and abroad. Most listed entities are groups based overseas. On which types of individuals and groups should Canada focus its listing efforts in the future?

What could be done to improve the efficiency of the listing processes and how can listing be used more effectively to reduce terrorism?

Do current safeguards provide an appropriate balance to adequately protect the rights of Canadians? If not, what should be done?

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## TERRORIST FINANCING

Canada has a stable, open economy, an accessible and advanced financial system, and strong democratic institutions. However, those seeking to raise, transfer and use funds for terrorism purposes try to do so by exploiting some of these strengths. In confronting the evolving challenges of terrorist financing, the Government must ensure that it does not compromise fundamental Canadian values.

Terrorist financing is a multi-faceted global phenomenon. Terrorists (individuals and groups) raise, collect and transfer funds across the globe to carry out attacks and finance day-to-day operations. They raise funds from criminal activities and from legitimate sources, such as donations or business profits. Terrorists use a variety of methods to move their funds. These include the formal banking system, international trade, money services businesses, informal money transfer systems, digital platforms, and the physical transportation of cash or certain high value goods, such as gold or precious stones.

Individuals also finance terrorist activities by raising money themselves to travel abroad for terrorist purposes or to purchase materials for attacks. Since funds are vital to terrorist organizations, depriving them of these funds is one effective mechanism to counter terrorism.

For example, one of the five priorities of the Global Coalition against ISIL is to reduce Daesh's capabilities by cutting off its access to funding. Daesh is likely the wealthiest terrorist group in the world, due to its access to proceeds generated in the territory it controls. Its wealth allows it to carry out attacks, recruit and pay members, provide training and indoctrination, maintain communications networks and disseminate propaganda. Reducing access to funds will diminish Daesh's capability.

### Canada's Approach to Counter Terrorist Financing

In Canada, the Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) regime involves 11 federal departments and agencies.<sup>24</sup> Together, they work to prevent, detect, deter, investigate and prosecute the financing of terrorist activities. A key component of Canada's regime is the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)*, which establishes FINTRAC.

The PCMLTFA imposes obligations on more than 31,000 financial service providers and financial intermediaries. The Act makes them active partners in the fight against money laundering and terrorist financing. Under the Act, these entities must keep certain records, know their customers, and report certain transactions to FINTRAC.<sup>25</sup> FINTRAC assesses entities' compliance with these

<sup>24</sup> Department of Finance, FINTRAC, the RCMP, the CBSA, CSIS, the Canada Revenue Agency, Department of Justice Canada, Public Prosecution Service of Canada, Public Safety Canada, Office of the Superintendent of Financial Institutions, and Global Affairs Canada.

<sup>25</sup> International electronic fund transfers (EFTs), cash transactions, disbursement from casinos over \$10,000; transactions suspected of being related to ML or TF; and terrorist property reports must be reported to FINTRAC.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

requirements and can fine them for non-compliance. FINTRAC also has the authority to analyze financial transaction reports and to disclose certain information to law enforcement and intelligence agencies if it has reasonable grounds to suspect that it would be relevant to the investigation or prosecution of a money laundering or a terrorist financing offence.

Law enforcement and intelligence agencies use this information and that from other sources to identify and disrupt terrorist activities. Law enforcement agencies can also lay criminal charges. The *Criminal Code* contains three terrorist financing offences. These prohibit (1) providing or collecting property for terrorist-related activities; (2) providing or making available property or services for terrorist purposes; and (3) using or possessing property for terrorist purposes. As noted earlier,<sup>26</sup> the *Criminal Code* also provides for a process to list individuals or groups as terrorist entities. The listing of a terrorist entity results in its property being frozen immediately. The property may then be seized and forfeited to the Government.

*Consider a scenario...*

Ms. L is a friend of Mr. A. She supports the 123 Group and wants to send it money abroad. Ms. L goes to a bank to send a wire transfer of \$11,000 to a country where it is known that 123 Group operates. Because the amount is more than \$10,000, the PCMLTFA requires the bank to report the transaction to FINTRAC. FINTRAC concludes that the transaction is suspicious (given its destination and other indicators) and provides the information to RCMP investigators.

### **Canada's Contribution to International Efforts**

Terrorist financing is a global problem that requires a well-coordinated, multilateral response. The Financial Action Task Force (FATF), of which Canada is an active member, is an international organization that sets standards for combating money laundering and terrorist financing, which ensures all members' AML/ATF regimes are held to the same criteria. The FATF monitors the implementation of these standards among its own 37 members and the more than 190 countries in the global network of FATF-Style Regional Bodies through peer reviews and public reporting. The FATF is currently evaluating Canada against these standards and is expected to finalize and publish the results in summer 2016.

As well, Canada works with international partners through fora such as the United Nations, the G7/G20 and the Counter-ISIL Finance Group. Canada also implements several UNSC Resolutions to freeze and seize the assets of persons and entities engaged in terrorism. In addition, Canada supports regions where there is a higher risk for terrorist financing, such as the Middle East and North Africa. Canada does this through technical assistance on counter-terrorist financing. This

---

<sup>26</sup> See chapter "Terrorist Entity Listing Procedures"

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

assistance is designed to strengthen the capacity of financial systems in these regions to prevent them from being exploited as vehicles for terrorist financing.

## Potential Impacts on *Charter* Rights

The current approach requires certain businesses to disclose private financial information to FINTRAC. FINTRAC may disclose it to law enforcement and intelligence agencies for investigation. This could impact privacy rights protected by section 8 of the *Charter*.

Because of the potential impact on section 8 privacy rights, the PCMLTFA has safeguards in place. For example, the Act prescribes the information that FINTRAC can receive and disclose. The PCMLTFA also identifies the law enforcement and intelligence agencies that can receive FINTRAC's financial intelligence. The Act also limits when FINTRAC can disclose information to these agencies. It must have reasonable grounds to suspect that the information would be relevant to the investigation or prosecution of a money laundering or a terrorist financing offence, or relevant to the investigation of threats to the security of Canada. FINTRAC is independent from law enforcement agencies and does not conduct investigations.

To ensure that the terrorist financing regime addresses emerging risks and maintains appropriate safeguards, Parliament reviews the PCMLTFA every five years. As well, the PCMLTFA requires the Privacy Commissioner of Canada to conduct a review of the measures taken by FINTRAC to protect information it receives or collects under the Act every two years. This is to ensure that FINTRAC protects the information it receives as part of its operations. The Privacy Commissioner reports the findings of the review to Parliament.

Finally, the Government continues to monitor its AML/ATF regime to ensure that it aligns with international standards and that it takes into consideration government policy priorities, including its impact on businesses and the rights of individuals.

## Challenges

Canada's financial sector has evolved significantly since the PCMLTFA came into force in 2001. The Act has been amended several times in the past fifteen years, but staying current in the changing financial environment presents challenges. Financial technology is changing rapidly. The regime needs to keep pace with evolving techniques of using new platforms for illicit fundraising or financial transfers. In addition, the reporting thresholds under the Act may be set too high in terrorism matters. Banks and other financial institutions do not need to report to FINTRAC any transactions below these thresholds unless they deem them suspicious. For example, the \$10,000 threshold for reporting international funds transfers may be appropriate for investigations involving money laundering, but terrorists often transfer much smaller amounts. Enhanced coverage of new technologies and a lower reporting threshold would provide more information for investigations.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

However, it would also increase the personal information collected by FINTRAC, and the number of businesses required to report.

*Consider a scenario...*

Ms. L sends \$3,000 to a member of the 123 Group outside Canada. As the transaction is below the \$10,000 threshold, it is not reported to FINTRAC. The business transferring the funds has no information causing it to consider the transaction suspicious and so does not notify FINTRAC of the transaction. FINTRAC has no information to pass on to law enforcement agencies through legislated reporting mechanisms. Had FINTRAC known about the transfer, the PCMLTFA would have allowed it to inform law enforcement if it had reasonable suspicion that the transaction was related to the financing of a terrorist activity.

Terrorists are adaptable and may exploit weaknesses to avoid detection, impeding Canada's efforts to reduce terrorist financing. In addition, terrorists can procure goods or services without actual transfers of funds, limiting detection through the financial system. Terrorists have also used financial professionals with no ties with or sympathies for the terrorists' cause to help move money and resources between countries.

Terrorist financing investigations require extensive resources and significant sharing of information within Canada and with other countries. Investigation and detection also require cooperation within the private sector and between the private and the public sectors. Effective partnerships require a clear understanding by both the public and private sectors of terrorist financing methods and trends, to better and more accurately identify suspicious behaviour. These challenges suggest that an approach that adapts to technological advances and strengthens partnerships between government and the private sector, may be the most effective way to deny terrorists the resources they need.

## What do you think?

The Government would like your views about how best to address gaps and other challenges in the regime.

What additional measures could the Government undertake with the private sector and international partners to address terrorist financing?

What measures might strengthen cooperation between the Government and the private sector?

Are the safeguards in the regime sufficient to protect individual rights and the interests of Canadian businesses?

What changes could make counter-terrorist financing measures more effective, yet ensure respect for individual rights and minimize the impact on Canadian businesses?

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## INVESTIGATIVE CAPABILITIES IN A DIGITAL WORLD

Evolving technology has changed the way Canadians communicate and live their lives. Canadians are increasingly active online. They may use multiple communications devices and a wide variety of tools such as email, Internet banking, instant messaging and various social media applications. This evolution provides enormous benefits for Canadian society, but criminals and terrorists can use these same technologies. Digital communications are now a fundamental tool for terrorism-related activities, including radicalization to violence, facilitation of travel for terrorist purposes, acquisition of funding and equipment, and even training for terrorist actions. The potential harm resulting from the exploitation of evolving technologies is not limited to national security. Traditional criminal activity – from planning violent crime to committing frauds – also relies on these technologies. New public safety challenges continue to appear via the Internet, such as the distribution of terrorist propaganda and child pornography, cyberbullying, and the “Dark Web” and its associated criminal marketplace.

Digital information is sometimes more important than physical evidence or intelligence in investigating national security threats, solving crimes and prosecuting offenders.

To protect Canadians from crime or threats to safety and security, Canada's law enforcement and national security investigators must be able to work as effectively in the digital world as they do in the physical. Law enforcement must also have the ability to cooperate effectively with their international partners who seek digital evidence from Canada to further their criminal investigations and prosecutions. The laws governing the collection of information and evidence have not, however, kept pace with the rapid advancements of digital technology in the last 20 years and the role technology plays in the lives of Canadians today. Whether information comes from more traditional sources or from within the increasingly complex digital landscape, investigators need access to that information to investigate threats to national security and criminal activity, and to cooperate with foreign partners in a timely manner.

The term “lawful access” has been used as an umbrella term to refer to certain legally authorized procedural powers and techniques, as well as criminal laws, which may come into play when national security and law enforcement agencies conduct investigations. The Government has attempted to ensure that investigative tools are adequate to deal with new forms and uses of technology. These efforts have included multiple public consultations on “lawful access”<sup>27</sup> and updating cybercrime

---

<sup>27</sup> These include the 2002-2003 Lawful Access Consultations, details of which can be found at [www.justice.gc.ca/eng/cons/la-al/index.html](http://www.justice.gc.ca/eng/cons/la-al/index.html).



*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

and cyberbullying laws through the *Protecting Canadians from Online Crime Act*.<sup>28</sup> Canada's digital environment, however, continues to change dramatically. More data has been created in the last five years than ever before. As we move forward, discussions of the investigative capabilities of law enforcement and national security agencies in a digital world must take into account technological advances, the legal context and the current threat environment.

## Potential Impacts on *Charter* Rights

Access by national security and law enforcement agencies to digital communications, information for investigative or intelligence purposes, or both, could impact the privacy rights protected by the *Charter*. Some aspects of the issues discussed here could also impact freedom of expression or the right against self-incrimination, also protected under the *Charter*.

These issues are complex. Each raises specific concerns about its intersection with considerations of security and individual rights, including privacy. International and economic considerations also come into play.

## Challenges

In the physical world, law enforcement and national security agencies use a variety of tools to collect information and evidence to further their investigations and to assist foreign counterparts. The *Criminal Code* and other statutes, such as the *CSIS Act* and the *Mutual Legal Assistance in Criminal Matters Act*, authorize the use of these tools. For example, investigators at a crime scene may look for physical evidence such as DNA, fingerprints, weapons or other items of importance that may relate to the crime. In the digital world, investigators use other tools to collect digital information and evidence. In the digital world, investigators may be looking for information and evidence (data) such as online addresses (website or IP addresses), the types of communication that took place, with whom, and for how long.

Law enforcement and national security agencies obtain access to such data as authorized by law. However, the legislation providing for certain investigative tools may not be adequate to deal with the complexity, diversity, and rapid pace of change in the digital world. Current challenges impacting investigative capabilities include the following:

- lack of consistent and timely access to **basic subscriber information** to help identify the subscriber to a communications service;

---

<sup>28</sup> Some of the measures introduced by this Act were new production orders that allow for authority to obtain tracking data, tracing communication, and transmission data, new powers for preservation of data, and the creation of a new offence for the non-consensual distribution of intimate images, known as “revenge porn.” The Act also introduced measures to adapt some existing investigative tools to current technology and aligned those changes with privacy safeguards and requirements for judicial oversight.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

- lack of consistent and reliable technical **intercept capability** on domestic telecommunication networks;
- diminished ability to investigate due to the use of **encryption**; and
- inconsistent **retention** of communications data.

These challenges are discussed in order below.

In addition, cyberspace is not easily bound by domestic borders and laws. Many communications service providers (CSPs) have no infrastructure or business presence in Canada, but provide Internet-based communications services. These providers operate in Canada but may fall beyond the reach of Canadian law. This can cause significant challenges and delays for law enforcement and national security agencies in acquiring the information necessary to advance investigations. It can also lead to critical intelligence and evidence being unobtainable.

## Basic Subscriber Information

*Consider a scenario...*

There is suspicion that Mr. A. has inspired Mr. M. to begin planning a terrorist attack in Canada with an unidentified person. Much of Mr. M's collaboration happens through exchanges over the Internet, such as through online forums.

As part of the investigation of this suspicious activity, a police officer wants to request the identity (basic subscriber information) related to a particular Internet Protocol (IP) address that has been involved in these online exchanges. However, to get the information from the Internet service provider (ISP), the officer would need a court order. The officer is in the early stages of the investigation and does not have enough information to meet the threshold for obtaining this court order, since getting an order requires more than suspicion that the activities are taking place. As a result, the officer is unable to pursue an investigative lead in a timely and effective manner.

“Basic subscriber information” (BSI) consists of basic identifying information that corresponds to a customer's telecommunications subscription. This can include name, home address, phone number, email address, and/or IP address. BSI does not include the contents of communications. BSI provides law enforcement and national security agencies with key information. This information is particularly useful at the outset of an investigation and may also be used to follow investigative leads. The information allows the police and national security agencies to identify an individual.

In 2014, in *R. v. Spencer*, the Supreme Court of Canada decided that the police could not request the name and address of a person in relation to his or her IP address where it would reveal intimate details of his or her anonymous online activities, except in an emergency situation or pursuant to a reasonable law. The Court concluded that the manner in which the police in this case obtained such information interfered with privacy interests protected by the *Charter*.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

Without specific legislation designed to permit access, law enforcement and national security agencies have had difficulty getting timely and effective access to BSI since the *Spencer* decision. As a result, law enforcement agencies have used tools already available in the *Criminal Code*, such as general production orders. These tools are designed for a larger search scope. They are meant for situations such as seeking the complete browsing history, medical records or financial history of an individual. Because of this a high degree of judicial scrutiny is necessary.

The use of these tools for BSI presents the following challenges, especially during early stages of an investigation:

- The information needed to apply for a court order -- for example, a general production order -- may not be available at the beginning of an investigation. The existing information may not attain the threshold required for a court to grant an order.
- The process to obtain a search warrant or a general production order can be slow and involve considerable work and resources. The process has requirements that may be disproportionate when the only information investigators are seeking is BSI, even if the requirements are proportionate in other situations involving greater privacy intrusions.

As a result of these challenges, key evidence may be lost and opportunities to prevent a crime from happening missed. A tool designed to access BSI specifically could, with appropriate safeguards, both enhance investigative capabilities and respect privacy interests.

Laws in many foreign jurisdictions specifically permit law enforcement and national security agencies to obtain BSI. In many cases, this can occur without prior judicial authorization (generally, obtaining BSI without prior judicial authorization is called administrative access). These foreign jurisdictions include the U.S., the UK, Australia, Germany, Sweden, Ireland, Denmark, Spain, Finland, the Netherlands and Norway.

The laws and regulations in these jurisdictions vary in how they limit and safeguard administrative access to BSI. Some jurisdictions give certain agencies access to BSI administratively but require other agencies to obtain judicial authorization first. In some cases, a general administrative scheme for obtaining BSI operates, but an order from a judge may be required under certain conditions. These conditions requiring a court order may include when BSI is stored as part of a data retention requirement, or when certain categories of BSI are sought, such as an IP address or other data unique to mobile cellular devices, such as an International Mobile Subscriber Identity (IMSI) number. Other limitations in getting administrative access to BSI include requirements for senior police officers to approve requests and limiting BSI access to certain types of crime, or including prosecutors in the process to obtain some types of BSI.

Any measures to address the need for consistent and timely access to BSI would have to take into consideration the investigative needs of law enforcement and national security agencies and the

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

impact of those measures on industry. The measures would also have to protect privacy rights in accordance with the *Spencer* decision.

## Interception Capability for Communications Services

Law enforcement and national security agencies intercept private communications under the *Criminal Code* and the *CSIS Act* to obtain communications when investigating certain crimes (as listed in the *Criminal Code*) or threats to national security. Each Act sets out procedures to obtain judicial authorization to use interception techniques. These procedures are designed to uphold privacy rights.

Law enforcement and national security agencies obtain the necessary court orders to intercept communications. However, in some cases CSPs may not be able to perform the interception because the technical capability to intercept communications has not been built into their infrastructure. This hinders investigations that are being pursued under judicial authorization. In turn, this can prevent law enforcement and national security agencies from fulfilling their mandates.

Canada does not impose a general legal requirement for CSPs to have interception capabilities on their networks. Many other countries do. Australia, the U.S., the UK and many other European nations require CSPs to have an interception capability. In the U.S., for example, the *Communications Assistance for Law Enforcement Act*, usually referred to as CALEA, imposes this obligation. The U.S. Federal Communications Commission website explains CALEA.<sup>29</sup> Because of CALEA, traditional voice switches in the U.S. today include an intercept feature.

*Continuing the scenario from above...*

The investigation has now proceeded to a point well beyond suspicion and the police have received an authorization from a judge to intercept the communications of Mr. M.

However, when the police contact the telecommunications service provider, they learn that the service provider has not built a capability to intercept communications into its infrastructure. The service provider cannot complete the work required to develop and implement this intercept capability before the authorization expires. As a result, the police miss out on obtaining key evidence, even though they had court authority to intercept the communications.

Several issues need to be taken into account when discussing whether to require CSPs to introduce intercept capability. These include the impact on privacy, the investigative needs of law enforcement and national security agencies, and how introducing requirements for intercept capability may affect the costs and competitiveness of industry.

<sup>29</sup> <https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance>

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## Encryption

Encryption converts a readable electronic message into an unreadable message. To decrypt the message (make it readable again), the reader must use one or more specific decryption “keys.” Encryption is widely regarded as a best practice to enhance security and protect privacy online. It is commonly used to protect individual messages, personal devices and transmission channels. Secure encryption is also vital to cybersecurity, e-commerce, data and intellectual property protection, and the commercial interests of the communications industry. Canada's policy on cryptography (established in 1998) underlines the importance of encryption to the viability, stability and growth of the economy and e-marketplace and encourages the use of encryption to protect privacy, personal information and data. Today, free encryption technologies and services are widely available. These include encryption that often operates without the users' knowledge or need to activate it. Encryption technologies may be built in to a user's communication service.

However, encryption technology also helps criminals and terrorists to avoid discovery, investigation and prosecution by making their communications unreadable to investigators. The international availability of encryption tools and the complexities of encryption make law enforcement and national security investigations more difficult. They also pose challenges for law enforcement working with foreign partners in fighting serious international crimes.

It is difficult to address the problematic use of encryption without also reducing its benefits. As a result, very few countries have proceeded to limit encryption through legislation in the interests of protecting law enforcement and national security agency capabilities. This is despite the challenges posed by encryption for law enforcement and national security agencies being well known. Encryption has been the subject of concern and discussion in many jurisdictions since the 1990s.

The UK is among the few countries to impose limits on encryption through law – in this case, the *Regulation of Investigatory Powers Act, 2000*. The Act gives legally authorized persons (such as law enforcement and national security agencies) the authority to serve notices on individuals or bodies requiring the disclosure of protected (for example, encrypted) information in an intelligible form. This can be done through decryption or disclosure of encryption keys that the person is believed to hold. These provisions have attracted controversy.

In the 1990s, a series of legislative initiatives (sometimes referred to as “Clipper Chip” proposals) were suggested in the U.S. to impose built-in decryption capabilities. These proposals were highly controversial and attracted vigorous opposition from privacy and civil liberties groups and from groups concerned about the potential damage to industry. None of these proposals became law. However, vigorous debate about encryption continues in the U.S., as do concerns of law enforcement about encryption. This was seen most recently in the controversy that arose when the U.S. government asked Apple to help it obtain information contained on a phone associated with the San Bernardino terrorist incident.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

*Continuing the scenario from above...*

The police were finally able to develop intercept capability and obtain court authority again to intercept the communications of Mr. M.

To avoid having his plans discovered, however, Mr. M had encrypted his communications, which were unreadable to the police as a result. In addition, the service provider advised the police that it could not help decrypt the communications. After months of investigative delays and despite court authority to intercept the communications of Mr. M, the police cannot read them to obtain potential evidence. As a result, Mr. M's communications remain protected from law enforcement.

Even when law enforcement or national security agencies can intercept a communication, with assistance from a service provider under a court order, the data that is obtained is often unreadable due to the layers of encryption that cannot be decrypted or otherwise removed. Encryption challenges also apply to the court-ordered production of historical data, such as email, text messages, photos and videos from lawfully seized smartphones, computer hard drives and other digital devices. Since encryption can be used by anyone, a private sector organization may not be able to help law enforcement and national security agencies decrypt communications because the organization might not have the technical ability to decrypt material encrypted by someone else.

No provisions specifically designed to compel decryption are found in the *Criminal Code*, the *CSIS Act* or in other Canadian laws. In other words, there is no law in Canada designed to require a person or organization to decrypt their communications.

Discussion about encryption and decryption must take into account the potential impact on the following:

- human rights, including privacy rights, freedom of expression, and the right against self-incrimination;
- the investigative needs of law enforcement and national security agencies;
- commercial interests, such as competitiveness and the protection of intellectual property;
- how compelling decryption could weaken existing IT infrastructure models and systems;
- cybersecurity; and
- e-commerce.

## Data Retention

“Data retention” refers to the general requirements to store certain elements of subscribers’ telecommunications data, such as telephone numbers dialed, call length, time of call, and Internet equivalents, for the purpose of supporting law enforcement and national security investigations. These data can provide key pieces of information and evidence. Data retention ensures that this

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

information will be kept for a specified period so that law enforcement and national security agencies can obtain this information with a warrant, if required for an investigation. To date, Canada has not pursued a telecommunications data retention requirement for law enforcement and national security purposes.

*Continuing the scenario from above...*

As part of its ongoing investigation, the police learn that Mr. M had used his mobile phone over three weeks in July 2015 to communicate with individuals linked to terrorist groups. The police seek a court order to obtain telecommunications data associated with Mr. M's mobile phone account. However, the company keeps records for business purposes only for nine months. As a result, the company has already deleted data from July 2015 and the data are not available to the police.

Parliament recently introduced *preservation* powers into the *Criminal Code* when it enacted the *Protecting Canadians from Online Crime Act*. These powers allow law enforcement agencies to seek a court order or demand the preservation of specific computer data belonging to specific persons for a brief time to assist in investigations.

However, some business practices are changing and companies are deleting data more quickly than before, sometimes before law enforcement can seek a court order for or demand preservation. In addition, the length of time data is held varies from company to company. General data retention requirements would provide for companies to keep data for a standardized period. However, this might mean that companies have to store data for longer than they require strictly for business purposes. Requiring data retention for a given period could also increase risks to personal information held by companies. The longer personal information is kept, the longer it is vulnerable to attack.

General requirements for data retention already exist in some foreign jurisdictions or have been proposed or debated there. In the U.S., some data retention bills have been introduced in Congress, but none have been enacted. Australia recently enacted data retention requirements. On March 15, 2006, the European Union (EU) issued a Data Retention Directive (DRD) to impose data retention requirements for telecommunications data on its member states.

The DRD required that data retention be implemented through legislation enacted by EU member states at the national level. The manner of the implementation varied significantly among member states, in part because of controversy over these requirements in some states. On April 8, 2014, the Court of Justice of the European Union struck down the DRD, calling it inconsistent with privacy rights in Europe.

EU member states are now looking at their respective national laws to determine if and how their national laws on data retention need adjustment after the court decision. Some countries, such as Germany, have already introduced changes. The Federal Constitutional Court of Germany declared

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

the country's own domestic legislation unconstitutional in March 2010. A new data retention law came into effect in Germany on January 4, 2016. The law introduced many safeguards, such as reducing the obligation to retain data from six months to ten weeks and restricting access to such data to cases involving “serious crimes” only.

The discussion of telecommunications data retention requirements should take into account several issues, including the following:

- the investigative needs of law enforcement and national security agencies;
- the impact on privacy interests; and,
- the impact on the costs and competitiveness of companies resulting from data retention requirements.

## What do you think?

How can the Government address challenges to law enforcement and national security investigations posed by the evolving technological landscape in a manner that is consistent with Canadian values, including respect for privacy, provision of security and the protection of economic interests?

In the physical world, if the police obtain a search warrant from a judge to enter your home to conduct an investigation, they are authorized to access your home. How should investigative agencies operate in the digital world?

Currently, investigative agencies have tools in the digital world similar to those in the physical world. As this document shows, there is concern that these tools may not be as effective in the digital world as in the physical world. Should the Government update these tools to better support digital/online investigations?

Is your expectation of privacy different in the digital world than in the physical world?

## Basic Subscriber Information (BSI)

Since the *Spencer* decision, police and national security agencies have had difficulty obtaining BSI in a timely and efficient manner. This has limited their ability to carry out their mandates, including law enforcement's investigation of crimes. If the Government developed legislation to respond to this problem, under what circumstances should BSI (such as name, address, telephone number and email address) be available to these agencies? For example, some circumstances may include, but are not limited to: emergency circumstances, to help find a missing person, if there is suspicion of a crime, to further an investigative lead, etc... Do you consider your basic identifying information identified through BSI (such as name, home address, phone number and email address) to be as private as the



*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

contents of your emails? your personal diary? your financial records? your medical records? Why or why not?

Do you see a difference between the police having access to your name, home address and phone number, and the police having access to your Internet address, such as your IP address or email address?

### **Interception Capability**

The Government has made previous attempts to enact interception capability legislation. This legislation would have required domestic communications service providers to create and maintain networks that would be technically capable of intercepting communications if a court order authorized the interception. These legislative proposals were controversial with Canadians. Some were concerned about privacy intrusions. As well, the Canadian communications industry was concerned about how such laws might affect it.

Should Canada's laws help to ensure that consistent interception capabilities are available through domestic communications service provider networks when a court order authorizing interception is granted by the courts?

### **Encryption**

If the Government were to consider options to address the challenges encryption poses in law enforcement and national security investigations, in what circumstances, if any, should investigators have the ability to compel individuals or companies to assist with decryption?

How can law enforcement and national security agencies reduce the effectiveness of encryption for individuals and organizations involved in crime or threats to the security of Canada, yet not limit the beneficial uses of encryption by those not involved in illegal activities?

### **Data Retention**

Should the law require Canadian service providers to keep telecommunications data for a certain period to ensure that it is available if law enforcement and national security agencies need it for their investigations and a court authorizes access?

If the Government of Canada were to enact a general data retention requirement, what type of data should be included or excluded? How long should this information be kept?

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## INTELLIGENCE AND EVIDENCE

National security information needs to be protected from unnecessary public disclosure. At the same time, there is a need to facilitate its use in legal proceedings, when appropriate, while maintaining the fairness of the proceedings and the integrity of the justice system.

The challenge is significant in criminal and related proceedings involving constitutionally protected interests. National security information might also, for example, be important in advancing or defending against a civil case. The Government might also use such information when making administrative decisions, which in turn can be judicially reviewed.

When national security information is involved—or potentially involved—in a legal proceeding, it brings into play issues of fundamental justice, the rule of law and the confidence of Canadians in the justice system. The potential disclosure of national security information may also limit the effectiveness of national security agencies and make it more difficult to assure foreign partners that national security information they have shared with Canada is protected.

### Key Principles

The discussion of intelligence and evidence raises several important principles, including the following:

- the requirement that laws be consistent with the *Charter* ;
- the obligation of the Government to protect sensitive sources, capabilities and techniques, and its relationships with international partners, in the interests of national security and international relations;
- the ability of courts and tribunals to consider as much relevant material as possible to ensure that judgments are based on a complete picture of the facts and that justice is done; and
- the need for legislative tools to be flexible enough to apply in a broad range of circumstances.

Section 38 of the *Canada Evidence Act* (CEA) provides the framework for the disclosure and use of national security information in a broad range of legal proceedings. Under section 38, a Federal Court judge must assess whether or not the disclosure would be injurious to international relations, national defence or national security. If disclosure would be injurious, the judge must then consider whether the public interest in disclosure outweighs the public interest in non-disclosure. The process under section 38 of the CEA is conducted in the Federal Court even though, for example, the information may relate to a proceeding in a different court.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

This two-part process, also known as a bifurcated process, has been the subject of criticism.

The Supreme Court of Canada concluded that this bifurcated approach is constitutional in a criminal proceeding (*R. v. Ahmad (2011)*). Still, the Court invited the Government to consider its policy choice of using a bifurcated system. The issues surrounding intelligence and evidence have also been addressed in a number of reports, including reports of parliamentary committees and the Air India Inquiry.<sup>30</sup> Intelligence and evidence has also been the subject of consultations in New Zealand and the UK.

Intelligence and evidence issues can be expected to continue to arise for several reasons, including that a number of federal agencies are involved in national security investigations. In some cases, the need for cooperation between federal institutions has resulted in an increasing number of government actions being informed by national security information.

## Criminal Proceedings

The Federal Court does not hear criminal cases, unlike the criminal courts in the provinces and territories. However, issues relating to the disclosure of national security information in these cases are largely addressed by Federal Court judges.

This means that, in some instances, the criminal court in a province may be unable to see the national security information and may only be able to rely on unclassified summaries provided by the Federal Court.

In other cases, the Attorney General of Canada, in consultation with investigating agencies, may allow disclosure in court of national security information under certain conditions, determined case by case. However, these proceedings are unable to incorporate the protections for national security information built into the *Canada Evidence Act*. Nor can they benefit from using the Federal Court's secure facilities or relying on its administrative expertise in handling national security information.

### *Consider a scenario...*

After a long investigation, the RCMP lay criminal charges in the superior court of the province against Mr. M for planning a terrorist attack. Information provided by CSIS was essential to the RCMP investigation. This information was obtained from a foreign agency, which provided it on condition that it not be further disclosed without the agency's consent. The foreign agency refuses to consent to the disclosure. Revealing this national security information without the foreign agency's consent would damage CSIS's relationship with it.

To protect against the disclosure of the information provided by the foreign agency, the Attorney General of Canada makes an application under the *Canada Evidence Act* for the Federal Court to decide whether it is in the public interest to protect or disclose the information. The Federal Court judge decides to protect the national security information, which means that the actual information

<sup>30</sup> Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

will not be given to the judge of the superior court or be relied on during the prosecution.

However, the judge of the Federal Court also decides to prepare an unclassified summary of the information, which is provided to Mr. M and the judge of the superior court. Mr. M uses this summary to defend himself against the charges and the judge of the superior court may consider it during the proceedings. Because this information is an important part of the prosecution's case, not being able to rely on the complete information in the superior court could cause the prosecution to fail.

National security agencies collect information to advise government, but the information is not generally intended to be used as evidence. In some circumstances, the obligation on the prosecutor to make disclosure in criminal cases may require the prosecutor to approach these agencies to see if they have information relevant to the case. The prosecutor must do this even if the agencies did not provide that information to law enforcement for the criminal investigation. This is one way for national security agencies to get drawn into criminal proceedings.

### Potential Impacts on Charter Rights

When trying to protect national security information in a criminal case, the Government must ensure that any measure to do so is consistent with the *Charter*.

An individual accused of a crime has a right to a fair trial, including the right to make full answer and defence. This involves broad access to information that relates to the investigation and charges. The accused also has a right to be present throughout the trial. Finally, the open court principle protected by the *Charter* may come into play when national security information is used in a criminal trial.

### Civil Proceedings

National security information may be relevant in a civil proceeding and can sometimes be central to a proceeding. Where national security information is involved, a plaintiff may be unable to make its case, and a defendant may be unable to defend itself, because the information needed to establish the case or defend against a claim needs to be protected. This situation can arise when the federal government is sued for allegedly wrongful conduct, when it is the plaintiff, or in proceedings where the federal government is not at all involved (for example, a dispute between two private companies).

If a judge is unable to take into account the national security information in the civil proceeding, justice may not be served. The lack of relevant information could lead to damage to someone's reputation, costly settlements or loss of public confidence in the legal system.

To protect the national security information from being disclosed to the court and non-governmental parties, the same bifurcated process under the *Canada Evidence Act* described for the criminal process above applies to civil proceedings.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## Potential Impacts on Charter Rights

Unlike criminal proceedings, civil proceedings do not automatically bring the *Charter* right to liberty into play. However, parties in civil proceedings generally have a right to documents that contain relevant information that either directly or indirectly advances or damages the case of one party or another. The protection of national security information from disclosure in a civil case could make it difficult to successfully pursue, or defend against, *Charter* claims.

## Administrative Proceedings

Many federal administrative decision makers might rely on national security information in their work. These decision makers include federal government officials, ministers, boards and administrative tribunals. The decisions involve a wide variety of matters, such as issuing or revoking permits or licences. For example, decisions about issuing passports are considered administrative proceedings.

As in criminal and civil proceedings, national security information must be protected in administrative and related proceedings, while at the same time the proceedings must ensure fairness. Section 38 of the *Canada Evidence Act* provides a general regime for protecting national security information in some of these situations. Challenges similar to those outlined in the criminal and civil contexts exist here as well.

Apart from section 38 of the *Canada Evidence Act*, a number of specific regimes, varying slightly in their procedures, allow for the protection and use of the national security information during proceedings. Immigration proceedings are one example.

## Potential Impacts on Charter Rights

Procedural fairness requirements vary depending on the nature of the administrative decision. The content of the duty of fairness, which includes the rights to know the case to meet and to respond in a meaningful way, varies depending on the rights and interests at stake. Even when *Charter* rights are significantly impacted, the right to know the case to meet is not absolute.

## Proceedings under the *Immigration and Refugee Protection Act* (IRPA)

In making immigration decisions, the Government must sometimes rely on classified information (that is, information that if disclosed would be injurious to national security or endanger the safety of a person) to determine whether foreign nationals and permanent residents may enter or remain in Canada (whether they are “admissible”). Division 9 of the IRPA allows the Government to protect and use this information during immigration proceedings. The best known of these Division 9 proceedings are commonly called security certificate proceedings.

The certificate is a document, signed by the Minister of Public Safety and Emergency Preparedness and the Minister of Immigration, Refugees and Citizenship. It states that there are reasonable

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

grounds to believe that the named person is inadmissible to Canada for reasons of security, violating human or international rights, serious criminality or organized criminality. The certificate is referred to a judge of the Federal Court to determine its reasonableness. The proceedings at the Court have two parts:

- (1) public proceedings, where the person named in the certificate, along with their counsel, receive non-classified information and an unclassified summary of the classified information that is part of the certificate; and,
- (2) closed proceedings, where the public, the person named in the certificate and their counsel are not present and a court-appointed special advocate (a private lawyer with an appropriate security clearance) receives the classified and non-classified information relevant to the certificate and protects the interests of the named person.

*Consider a scenario...*

Ms. N is a permanent resident currently in Canada. CSIS has classified information from sources within Canada, as well as from an international partner, that shows Ms. N is part of a terrorist group and a danger to the security of Canada. She has been attending Mr. A's meetings. CSIS provides this information to the Minister of Public Safety and Emergency Preparedness and the Minister of Immigration, Refugees and Citizenship. The ministers decide to sign a security certificate and a warrant for her arrest. The certificate and warrant are filed with the Federal Court. The security certificate process protects the classified information from being disclosed while allowing it to be used by the Federal Court judge, who must determine if the certificate is reasonable.

### Potential Impacts on Charter Rights

A person's rights under the *Charter* are engaged by security certificate proceedings. These include the right not to be deprived of liberty and security of the person, except in accordance with the principles of fundamental justice. These principles include the right to a fair hearing, and the right to know the case to meet and to answer that case.

To protect these rights, the law provides certain safeguards. During closed proceedings, special advocates protect the interests of the person named in the certificate. They can challenge government claims that information cannot be disclosed, as well as the relevance, reliability and sufficiency of the information and evidence in the case. Special advocates can make submissions to the Court, cross-examine witnesses during the closed proceedings, and exercise any other power the judge authorizes.

Also, whenever a person is subject to detention or conditions under a warrant, the Court reviews this detention or these conditions on a regular basis (at least once every six months).

Finally, judges ensure the fairness of these proceedings and decide whether the security certificate is reasonable. The Supreme Court of Canada, in the *Harkat* decision, stated that the "judge is intended to play a gatekeeper role, is vested with broad discretion and must ensure not only that the record

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

supports the reasonableness of the ministers' finding of inadmissibility, but also that the overall process is fair.”<sup>31</sup>

The ATA, 2015 changed three aspects of Division 9 of IRPA proceedings (e.g. security certificates):

- The Government can immediately appeal when a judge orders the public disclosure of information that the Government considers must remain classified;
- The information that the ministers must file with the Federal Court is that which is relevant to the ground of inadmissibility on which the certificate is based and which allows the person to be reasonably informed of the case; and,
- The Government may ask the judge for an exemption from providing some classified information to the special advocate (as part of the disclosure of relevant information in closed proceedings). The judge may grant this exemption only if satisfied that the exempted information would not enable the person to be reasonably informed of the Government's case. The judge is permitted to consult with the special advocates about the information before making this decision.

*Continuing the scenario from above...*

During the security certificate process for Ms. N, the Federal Court judge decides that some of the classified information should be disclosed publicly. The Government appeals this decision immediately because releasing this information would harm national security. The Federal Court of Appeal reviews the decision to disclose the information. The Federal Court of Appeal decides to protect the information and the case continues without it being disclosed.

## What are other countries doing?

Australia, New Zealand, the UK and the U.S. face the same challenges of handling intelligence and evidence in their court systems. In criminal matters, for the most part, courts work from legislated roadmaps to protect national security information and maintain an adversarial legal system.

In general, Australia and the U.S. allow private (non-government) counsel to be security-cleared and have access to national security information in representing their clients. New Zealand and the UK have developed surrogates: special counsel acting as alternatives to disclosure of the national security information to the person involved.

In civil litigation involving the potential disclosure of national security information, some countries differ if national security information is sought to be used as evidence. In the U.S., a legal concept known as the common law State Secrets Privilege has evolved. This permits hearings behind closed

<sup>31</sup> *Canada (Citizenship and Immigration) v. Harkat*, 2014 SCC 37.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

doors without the affected person or the person's counsel being present which can result in the summary dismissal of claims based on the potential disclosure of state secrets. Elsewhere, including in Australia, procedures established by legislation allow for the substitution of national security information with summaries, admissions of fact or limited disclosure (where possible). Finally, the UK has legislated closed civil proceedings where the judge may review and rely on national security information tendered in closed proceedings, with the interests of the non-government party represented by a special advocate.

Senior administrative tribunals in Australia, the UK and New Zealand consider complaints involving security agencies as a part of their broad supervisory roles. Given their mandate, these senior administrative tribunals involve sitting judges.

### **What do you think?**

Do the current section 38 procedures of the *Canada Evidence Act* properly balance fairness with security in legal proceedings?

Could improvements be made to the existing procedures?

Is there a role for security-cleared lawyers in legal proceedings where national security information is involved, to protect the interests of affected persons in closed proceedings? What should that role be?

Are there any non-legislative measures which could improve both the use and protection of national security information in criminal, civil and administrative proceedings?

How could mechanisms to protect national security information be improved to provide for the protection, as well as the reliance on, this information in all types of legal proceedings? In this context, how can the Government ensure an appropriate balance between protecting national security and respecting the principles of fundamental justice?

Do you think changes made to Division 9 of the IRPA through the ATA, 2015 are appropriately balanced by safeguards, such as special advocates and the role of judges?



*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## CONCLUSION

Canada, like other countries, faces national security threats. The threat of terrorism, by global and by domestic actors, is real and evolving. More people are radicalizing to violence. Some are leaving Canada to join terrorist groups overseas, while others focus their attention on Canada itself. Canadians expect the Government to keep them safe. At the same time, the Government must comply with the rights enshrined in the *Charter*.

The issues described in the Green Paper and this background document relate to major components of our counter-terrorism framework. Some chapters discuss measures already in place. Certain chapters highlight current gaps, while others explain where the Government would like to take action. We hope that this information helps Canadians understand this complex area as we begin consultations with them about how best to respond.

Government counter-terrorism actions undoubtedly impact rights protected under the *Charter*.

Views will differ on what are justifiable and reasonable impacts. There will also be strong opinions on the tools we should employ and how they should be employed.

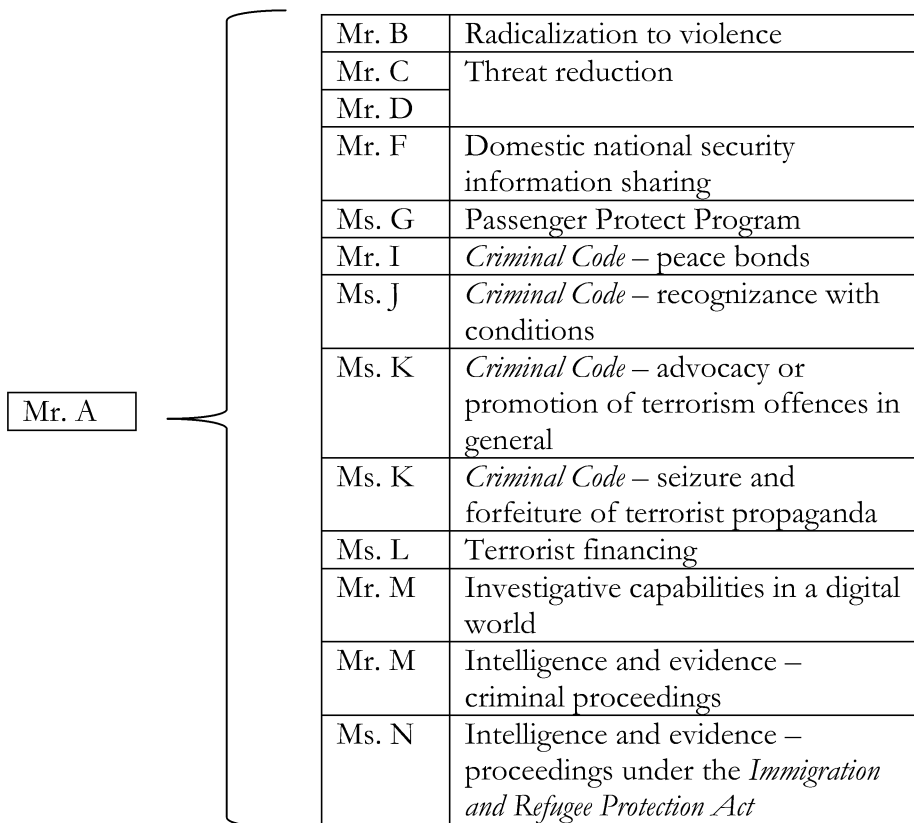
The views of Canadians about these issues – issues affecting us all – will help inform the Government as it designs the most appropriate mechanisms to deal with the evolving terrorism threat facing Canada.

Thank you for taking the time to read through this paper and for providing your thoughts.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## ANNEX – DIAGRAM OF SCENARIO CHARACTERS

The chart below demonstrates Mr. A's links to his followers, and which ones are discussed in various chapters in the document.



There are also two other individuals, who are not associated to Mr. A, but who appear in some chapters.

Ms. E	Domestic national security information sharing
Mr. H	Passenger Protect Program



Commissariat  
à la protection de  
la vie privée du  
Canada

Office of the  
Privacy  
Commissioner of  
Canada

Designation / Classification Désignation sécuritaire / Security Classification	Pages totales Total Pages
UNCLASSIFIED	4 + attachments

---



---

## NOTE D'INFORMATION

## BRIEFING NOTE

---



---

### Public Safety's National Security Consultations

**OBJET / PURPOSE:** To clarify how the Office will participate in the recently-launched Government consultations on National Security.

**ENJEU / ISSUE:** On September 8, 2016, Public Safety Canada launched a consultation exercise with the overarching objective of “[being] effective in keeping Canadians safe [and] to safeguard our values, our rights and freedoms, and the open, inclusive and democratic character of our society”<sup>1</sup>

**CONTEXTE / BACKGROUND:** These consultations, which close December 1, 2016, follow the format Public Safety has implemented for the ongoing Cyber Security consultations, namely, participants are invited to react to a consultation document (appended for reference) which will inform the discussion.

During the press conference for the launch, Public Safety Minister Goodale indicated that the government intended to fulfill its election promise to “repeal the problematic elements of C-51”<sup>2</sup> by undertaking the following:

- Ensuring everything done in the national security area complies with the Charter;
- Protecting lawful advocacy, protest and dissent;
- Establishing a more precise definition of propaganda;
- Ensuring appropriate treatment of appeals by individuals on no-fly lists; and,
- Revisiting the *Anti-Terrorism Act, 2015* (Bill C-51) after three years.

Above and beyond committing to undertaking these five changes, Public Safety is soliciting broad, public engagement focusing on the following ten key topic areas described in the consultation document:

#### 1. *Accountability*

Existing accountability mechanisms are outlined, including Ministerial Oversight, the Judiciary, expert review (i.e. SIRC, OCSEC and CRCC), Parliament (including the National Security and Intelligence Committee of Parliamentarians as proposed by C-22), Agents of Parliament (i.e. the OPC, Information Commissioner and Auditor General) and Commissions of Inquiry (i.e. O'Connor, Major and Iacobucci)

---

<sup>1</sup> Our Security, Our Rights: National Security Green Paper, 2016 (7777-6-162823, page 21)

<sup>2</sup> Liberal Party Platform 2015: A New Plan for a Strong Middle Class (7777-6-107445, page 53)

2. *Prevention*

The consultation document describes paths to radicalization, as well as ongoing initiatives by the RCMP and Correctional Services Canada to identify and counteract those at risk of being radicalized. Various additional strategies, including community outreach and youth engagement, are proposed for discussion.

3. *Threat Reduction*

The consultation document describes how CSIS operates to identify and engage other departments or agencies on threats to the security of Canada. A quick discussion follows of the new powers given to CSIS by C-51 (i.e. the so-called "kinetic" powers of threat disruption) as well as an explanation of thresholds necessary for investigation and risk assessment measures.

4. *Domestic National Security Information Sharing*

The challenges of interdepartmental information sharing are outlined, as well as a reference to government's obligations under the *Privacy Act*. A brief mention of the new powers to share information related to activities "that undermine the security of Canada" as enacted under the *Security of Canada Information Sharing Act* is included.

5. *Passenger Protect Program*

The consultation document includes a description of the no-fly list, as well as the *Secure Air Travel Act* as passed by C-51. Of note is the commitment to "introduce a new, more efficient and effective redress program" to address the issue of false positives.

6. *Criminal Code Terrorism Measures*

The consultation document describes the amendments made to the *Criminal Code* by C-51 regarding terrorist offences, as well as an outline of recognizance with conditions and terrorism peace bonds. Furthermore, the document includes a description of promotion of terrorism offences, seizure of terrorist propaganda (as well as CBSA's role therein) and witness protection measures put in place by C-51.

7. *Terrorist Entity Listing Procedures*

The document explains what a "listed entity" is, outlines how an entity is listed and what the ramifications of such a list are.

8. *Terrorist Financing*

Common methods of terrorism financing are described, as are financial institutions obligations to thwart these practices. Of interest is that neither FINTRAC nor the *Process of Crime (Money Laundering) and Terrorist Financing Act* are mentioned by name.

**9. Investigative Capabilities in a Digital World**

The document illustrates the evolving threats of the digital world, and the challenges of balancing privacy and security.<sup>3</sup> Of particular interest are the areas of basic subscriber information, intercept capability, encryption and data retention.

**10. Intelligence and Evidence**

The list concludes by describing the challenge of using evidence gathered in the course of intelligence work being used in civil, criminal or immigration proceedings.

The document concludes with a series of questions designed to inform the discussion, including how accountability can be strengthened, and how radicalization can be prevented, how safety and security can be achieved while balancing rights and freedoms.

**CONSIDÉRATIONS STRATÉGIQUES / STRATEGIC CONSIDERATIONS:**

There is much in this document upon which we can provide useful comment, including Accountability, Domestic Information Sharing, Passenger Protect, Terrorist Financing and Investigative Capabilities in a Digital World. A larger piece encapsulating our concerns in the entire national security and intelligence area writ large would be a useful addition to the discussion, and would help to clarify our ongoing concerns.

**MESURES RECOMMANDÉES / RECOMMENDED ACTION:**

That we prepare an outline of a formal response to this call for consultation for your approval.

**RELATED DOCUMENTS / DOCUMENTS CONNEXES:**

- Public Safety consultation workbook: Our Security, Our Rights (7777-6-162823)

**DISTRIBUTION:** Commissioner, LSPRTA, DG *Privacy Act* Investigations, DG PIPEDA Investigations, DG Audit and Review, DG of Communications

**APPROBATION / APPROVAL:**

<b>Rédigé par / Prepared by</b> Leslie Fournier-Dupelle	<b>Date</b> September 8, 2016	<b>Revisions</b>
<b>Approuvé par / Approved by</b>  Barbara Bucknell <i>Directrice, Politiques et recherche / Director, Policy and Research</i>		

<sup>3</sup> Of interest is that this key topic is very similar to the theme of "Policing in Cyberspace", raised by Public Safety Canada in their Cyber Security consultation workbook (7777-6-160126, page 9).

Approved by – Approuvé par	Date
Patricia Kosseim <i>Avocate générale principale et Directrice générale / Senior General Counsel</i>	
Approuvé par / Approved by	Date
<input type="checkbox"/> Je suis satisfait des mesures proposées. / I agree with the proposed recommendation(s). <input type="checkbox"/> Je ne suis pas satisfait de ces recommandations pour les raisons suivantes. / I do not agree with the proposed recommendation(s) for the following reason(s):	
Commentaires ou des instructions supplémentaires / Additional Comments or Instructions:	
Daniel Therrien <i>Le commissaire à la protection de la vie privée / Privacy Commissioner</i>	



# Our Security, Our Rights

## National Security Green Paper, 2016

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.



Government  
of Canada

Gouvernement  
du Canada

Canada





*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

# Our Security, Our Rights: National Security Green Paper, 2016

---

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## MESSAGE FROM THE MINISTERS

A fundamental obligation of the Government of Canada is the responsibility to protect our safety and security at home and abroad. Equally fundamental is the responsibility to uphold the Constitution of Canada, and to ensure all laws respect the rights and freedoms we enjoy as people living in a free and democratic country.

When former Bill C-51, the *Anti-terrorism Act, 2015* (ATA, 2015), was tabled in the House of Commons, many Canadians voiced concern with the Government's approach to these responsibilities and whether the proposed legislation appropriately safeguards both security and rights. Those concerns have not diminished since the passage of the ATA, 2015.

The Government is committed to openness, transparency, and accountability. An early demonstration of this commitment was making public the Prime Minister's mandate letters to Ministers, so that Canadians could see our full list of priorities. Reflecting the seriousness with which the Government regards the concerns about the ATA, 2015, our mandate letters direct us to work together to repeal its problematic elements and introduce new legislation that strengthens accountability and national security. In this respect, we have made commitments to:

- guarantee that all Canadian Security Intelligence Service (CSIS) warrants comply with the *Canadian Charter of Rights and Freedoms* (the *Charter*);
- ensure all Canadians are not limited from legitimate protest and advocacy;
- enhance the redress process related to the Passenger Protect Program and address the issue of false positive matches to the list;
- narrow overly broad definitions, such as defining "terrorist propaganda" more clearly; and
- require a statutory review of the ATA, 2015 after three years.

In addition, we are establishing a statutory national security and intelligence committee of parliamentarians with broad access to classified information to examine how national security institutions are working. Further, we are also launching the Office of the community outreach and counter-radicalization coordinator to provide national coordination on preventing radicalization to violence; work with partners across communities, provinces, stakeholders and experts to ensure community resiliency; and, to develop a national strategy involving programming, policy and research.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

These are our commitments thus far, but we know more can be done. We do not view this as a simple exercise of repealing some legislative provisions and enacting new ones. Our aim is to ensure that the right tools are available to law enforcement and security officials, that they are appropriate, and that they are in keeping with Canadian values.

We consider this as an opportunity to engage you and your fellow Canadians in a discussion about certain aspects of our country's national security framework. This discussion is necessary if Canadians are to be appropriately informed about national security matters and empowered to contribute to – and influence - elements of that framework.

This Green Paper has been prepared to facilitate the process of providing us with your views. It will also serve as the foundation for the consultation that will take place in the coming months.

We sincerely hope that you will take the time to read this material and join in this discussion. We look forward to your contributions to what, we are sure you will agree, is a timely and truly important national initiative. Together we can ensure that the Government appropriately achieves a framework that upholds both security and rights.

Hon. Ralph Goodale, P.C., M.P.  
Minister of Public Safety  
and Emergency Preparedness

Hon. Jody Wilson-Raybould, P.C., M.P.  
Minister of Justice and  
Attorney General of Canada

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## INTRODUCTION

In Canada, we are not isolated from the terrorist threat. Since the 2001 *Anti-terrorism Act*, threats to our domestic and international security have continued to evolve.

New terrorist groups – including the so-called Islamic State of Iraq and the Levant (ISIL) – have emerged and engineered chaos and destruction in many parts of the world. What has been referred to as ISIL will be referred to as Daesh in this document. Increasing numbers of Canadians have travelled to the Middle East to join terrorist organizations, including Daesh. And extremist narratives have motivated a number of Canadians to plot and pursue attacks against domestic targets.

Indeed, the principal terrorist threat to Canada remains the possibility of violent extremists carrying out attacks within our borders.

Our national security institutions share a duty to keep Canadians safe – and they do so daily. At the same time, these agencies are themselves subject to measures to keep them accountable to Canadians and ensure that the rule of law is respected.

In a world of uncertainty, risk and rapid change, do we have the tools necessary to keep people safe – and are we using all our tools in ways that also safeguard our values?

The Government urges Canadians to use this consultation process to be active partners in revamping our national security framework. We want policies that are more informed and better reflect the nature of the country we share.

Counter-terrorism efforts represent a complex and deeply charged area of public policy. People have strong perspectives and clear opinions, as they should on matters of such importance.

Each of the following chapters briefly outlines the issues at hand and gives a sense of the relevant challenges. Other documents available online – including an expanded background document – provide more detailed, technical information on issues.

You are invited and encouraged to respond online and share your views on this Green Paper and the associated documents. Your input will be welcomed until December 1, 2016 – at which point the government will begin the process of crafting new legislation, policy options and / or programs.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

We have before us the opportunity to build the national security framework we want for our country – a framework that reflects Canadian values and priorities, and the nature and character of who we are and how we want to live in the world. Let us begin.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## ACCOUNTABILITY

To protect our national security, a number of government agencies are given the power to collect intelligence and enforce laws. Much of this work is very sensitive and confidential.

We must make certain that a system is in place to ensure the accountability of these agencies. That is how Canadians will know that our intelligence and law enforcement powers are being exercised with great care, in a way that respects the *Charter*.

### Ministerial Oversight

In addition to the Prime Minister, two ministers in particular have important responsibilities related to national security and intelligence gathering:

The Minister of Public Safety and Emergency Preparedness is responsible for the Canada Border Services Agency (CBSA), the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), and Public Safety Canada.

The Minister of National Defence is responsible for the Communications Security Establishment (CSE), the Department of National Defence and the Canadian Armed Forces.

All Ministers are directly accountable to Parliament for the activities of their agencies.

### The Judiciary

Courts play an important role in national security.

For example, they rule on whether a warrant will be issued to allow the use of intrusive powers to investigate a threat. That is one way of ensuring that our security efforts respect the *Charter*.

The courts also examine and judge whether the methods used to secure arrests and prosecutions were justifiable and proper. And they have the authority to provide remedies in appropriate cases in relation to law enforcement misconduct.

### Independent Review

There are independent, non-partisan review bodies that scrutinize the activities of certain government agencies. Their task is straightforward: to ensure that our national security and intelligence agencies operate:

- within the law; and
- in compliance with the directions set out by their Ministers.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

There are three such review bodies:

- The Civilian Review and Complaints Commission (CRCC), which is responsible for reviewing the RCMP;
- The Security Intelligence Review Committee (SIRC), which reviews CSIS;
- The Office of the Communications Security Establishment Commissioner (OCSEC), which reviews the CSE.

All three review bodies have a mandate to review activities and hear complaints. Each produces an annual public report that summarizes its activities.

## **Parliament**

Parliament holds Ministers to account for the actions of the agencies they oversee. It also considers, debates and votes on legislation relating to national security matters.

House of Commons and Senate committees can also examine policy issues related to national security, and conduct studies of government activities and existing or proposed legislation.

Currently, most Parliamentarians do not have access to classified information, which limits their ability to fully examine national security issues. The Government has therefore committed to creating a new national security and intelligence committee made up of Parliamentarians who will be given broad access to classified material.

## **Agents of Parliament**

Certain “agents of Parliament” have the authority to scrutinize national security activities.

The Privacy Commissioner, for instance, can examine how personal information is handled. The Information Commissioner can investigate complaints regarding access to information requests. And the Auditor General can conduct “value-for-money” audits on national security programs.

## **Commissions of Inquiry**

Commissions can be established to impartially investigate issues of national importance. Over the past decade, three separate Commissions of Inquiry have examined certain national security agencies. The three Commissions of Inquiry are:



*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

- The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar;
- The Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin; and,
- The Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

## PREVENTION

In recent years, we have all become familiar with the concept of “radicalization to violence.” It is a process whereby a person or group of people adopts a belief or ideological position that moves them toward extremism, violence and, ultimately, to terrorist activity.

It is not a crime to be a radical, nor to have radical thoughts or ideas. But as a society, our goal must be to prevent violence of all kinds, including violence committed in the name of radical ideologies or beliefs, and activities that support such violence such as facilitation and financing.

To do this, we must better understand how and why violent radicalization typically takes root. And we must ask ourselves: What more can we do to prevent people from becoming radicalized to violence?

Here is what we know:

- Family members and friends are often the first ones aware of an individual's first steps down the path of radicalization to violence – and may be in the best position to steer them away.
- Radicalization to violence is often driven by “narratives” that reduce global events to a few simplistic ideas.
- It frequently takes place within networks and communities, both physical and virtual (the Internet often plays a critical role).
- Radicalization to violence can be incited by friends, mentors or other influential individuals.
- Association with radicalized people can influence others to adopt a similar perspective.

### What Are We Currently Doing?

In the Government of Canada, a number of agencies play a role in addressing radicalization to violence:

- The RCMP trains officers on how to recognize early warning signs of radicalization. It also leads interventions in an effort to divert those on the path to violence.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

- Correctional Service Canada conducts tailored interventions for individuals in prison who have radicalized to violence, or are at risk of doing so.

## **What More Can We Do?**

The Government is dedicating \$35 million over five years to create an office for community outreach and countering radicalization to violence.

Activities to be supported by this office could include:

- **Working with Communities:** Empowering local leaders to strengthen community resilience and develop early intervention programs can be an effective way of preventing radicalization to violence.
- **Youth Engagement:** Radicalization to violence is, in Canada, disproportionately common among young people - it is important to reach out and support youth in ways that are meaningful to them.
- **Alternative Narratives:** Promoting positive alternative narratives through credible voices is one way to diminish the influence of violent, radical messages.
- **Emerging Research:** By engaging academics, think tanks and other Canadians, we can collect best practices and ensure the most effective means are being used to counter radicalization to violence. Knowing what works will help inform future policy in this area.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## THREAT REDUCTION

Here is how our system has worked for the past 30 years:

- CSIS collects information on suspected threats to the security of Canada and Canadians, at home and abroad.
- CSIS advises other agencies of government – law enforcement, for example – about the threats.
- These other agencies act on the information.

When Bill C-51 (the *Anti-terrorism Act, 2015*) was passed, CSIS was given a new mandate to take direct action to reduce threats to the security of Canada. This is known as “threat reduction,” or “disruption.” These threats are defined in the *CSIS Act* and have remained unchanged over the past 30 years.

To be clear: CSIS cannot arrest people. But it now has the authority to take timely action to reduce a threat – disrupting financial transactions, for instance, or interfering with terrorist communications.

To investigate, CSIS needs to have reasonable grounds to suspect that an activity is a threat. For threat reduction measures, CSIS has a higher threshold – it must have reasonable grounds to believe that an activity is a threat.

All threat reduction measures must be reasonable and proportional in the circumstances, and are subject to explicit restrictions. According to direction from the Minister of Public Safety and Emergency Preparedness, CSIS must also perform a risk assessment – and consult law enforcement and other agencies, as appropriate – for each threat reduction measure.

Depending on the actions it plans to take, the law requires that CSIS might have to get a warrant to proceed, especially if the measures would potentially affect the rights of Canadians as enshrined in the *Charter*.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## DOMESTIC NATIONAL SECURITY INFORMATION SHARING

National security threats can emerge and evolve quickly. Information must be gathered and shared among government agencies to ensure a full understanding of a potential threat, as various agencies can have different pieces of the full picture.

There are rules in place that affect the Government's authority to share information, especially information that may impact on individuals' privacy rights.

However, these rules are complex. It is sometimes difficult for one agency to know whether it can share information with another agency, and in some cases, there is no authority to share. This can affect our awareness of, and response to, an emerging national security threat.

Here is some important background: The *Privacy Act* governs the Government's management of personal information, including its collection, use and disclosure. Disclosure is not permitted without the consent of the individual to whom the information relates, other than in certain circumstances, some of which may apply to national security information sharing.

For example, the Department of Immigration, Refugees and Citizenship Canada will share with CSIS some personal information of applicants for permanent resident status in our country. This allows for more efficient and effective security screening.

### *The Security of Canada Information Sharing Act*

Bill C-51 (the *Anti-terrorism Act, 2015*) created the *Security of Canada Information Sharing Act* (SCISA), which established an additional authority for national security information sharing. It provides all federal government institutions with a new, explicit authority to disclose information related to an "activity that undermines the security of Canada" to certain designated federal institutions with national security responsibilities.

Importantly, this does not include activities of protest, advocacy, dissent or artistic expression. Information about these activities cannot be disclosed under the SCISA.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## THE PASSENGER PROTECT PROGRAM

Protecting air travellers is a key responsibility of the Government of Canada. We must also confront the threat posed by individuals who travel abroad – to countries such as Syria and Iraq – to engage in acts of terrorism.

These individuals can be involved in training, fundraising and other activities on behalf of terrorist groups such as Daesh. There is also the risk that, upon returning to Canada, these people may launch or inspire attacks here.

Under the new *Secure Air Travel Act* (SATA), which came into being with the passage of Bill C-51, the Government can use the Passenger Protect Program (PPP) – an air passenger identity screening program – to identify individuals who pose a threat to transportation security or are seeking to travel to commit certain terrorism offences.

These people are placed on what is known within the Government as “the SATA list” (casually referred to as a “No Fly List”).

Individuals on this list may be subjected to a range of measures to mitigate the threat that they pose, including being denied boarding of an aircraft – or having to undergo additional screening measures.

The list must be reviewed every 90 days to ensure there are still reasonable grounds to suspect an individual poses a threat.

Anyone who is denied boarding of an aircraft has the right to apply to the Minister of Public Safety and Emergency Preparedness to be removed from the SATA list and, if unsuccessful, to appeal the decision to the Federal Court.

False positive matches sometimes occur. This can result in air travel delays. The Government has made a commitment to introduce a new, more efficient and effective redress program to address the issue of false positive name matches to the SATA list.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## CRIMINAL CODE TERRORISM MEASURES

Since 2001, a number of people have been convicted of terrorism offences in Canada. Some have received life sentences. Our *Criminal Code* sets out a range of anti-terrorism powers for law enforcement and lists a range of terrorism-related offences.

With the *Anti-terrorism Act, 2015*, the *Criminal Code* was amended to:

- make it easier to prevent the carrying out of terrorist activity or terrorism offences;
- make it a crime to advocate or promote terrorism offences;
- give courts the power to order the seizure and forfeiture or removal of terrorist propaganda;
- give additional protection to witnesses and other participants in national security proceedings.

Let us look at each of these amendments, one by one.

### Reasonable Conditions

Generally, Canadian criminal law focuses on the prosecution of offences that have already taken place. But courts can also impose reasonable conditions on an individual in an effort to reduce the risk of that person committing an offence.

When it comes to potential terrorism, law enforcement has two tools at its disposal that it may use with the approval of a judge:

- **Recognizance with conditions**, which allows police to intervene and seek to have the court impose conditions on an individual who is suspected of being connected in some way to terrorist activity.
- A **terrorism peace bond**, which is used to prevent an individual from committing a terrorism offence, such as leaving Canada to commit an offence for a terrorist group.

With the passage of Bill C-51, it became easier for police to apply for, and use, these two tools.

For example, the thresholds to obtain a **recognizance with conditions** was lowered to apply to instances in which law enforcement officials believe terrorist activity “may be carried out” and suspect that the recognizance “is likely to prevent” it – rather than the previous thresholds of “will be carried out” and “is necessary to prevent”.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

And a **terrorism peace bond** can now be issued where law enforcement believes an individual “may commit” - rather than “will commit” - a terrorism offence.

People who are subject to a **recognizance with conditions** or a **terrorism peace bond** face the possibility of detention and other restrictions on their liberty, without having been charged with, or convicted of, an offence.

## Promotion of Terrorism Offences

It is now a criminal offence for a person to knowingly advocate the commission of terrorism offences in general. The individual *must know* that an offence will be committed or *be reckless* as to whether an offence may be committed as a result of what they say or write.

## Seizure and Forfeiture of Terrorist Propaganda

There are two new warrants in the *Criminal Code* that allow police to seize terrorist propaganda. This is material that encourages the commission of a specific terrorism offence, or terrorism offences in general. This material can be in printed, audio or video form, or it can be in electronic form on the Internet.

Related amendments to the *Customs Tariff* also allow CBSA border services officers to seize terrorist propaganda being imported into Canada without a warrant, as they would other contraband.

## Protection of Witnesses and Other Participants in the Justice System

Under the *Anti-terrorism Act, 2015*, enhanced measures are now available to protect witnesses and other participants in national security-related proceedings.

For example, judges can now order that witnesses testify behind a screen to conceal their identity, or use a pseudonym, or wear a disguise. And there is a broader range of instances under which charges can be laid against those who attempt to intimidate justice system participants.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## PROCEDURES FOR LISTING TERRORIST ENTITIES

Formally listing an individual or group as a “terrorist entity” is a way of curtailing their support and publicizing their involvement with terrorism.

The most common method of listing is available through the *Criminal Code*. An individual or group listed as a terrorist entity under the *Criminal Code* has its funds immediately frozen, and potentially seized and forfeited.

There are currently more than 50 terrorist entities which have been listed in this way. They include al-Qaida, the Taliban, Daesh, Boko Haram and more.

### How Does a Group Get Listed?

It begins with an investigation by the RCMP or CSIS. The Minister of Public Safety and Emergency Preparedness may then recommend to Cabinet that the entity be listed, so long as there are reasonable grounds to believe that the entity:

- knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity;  
or
- is knowingly acting on behalf of, at the direction of, or in association with an entity that has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity.

Many of Canada's closest allies keep similar lists of terrorist entities.



*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## TERRORIST FINANCING

Terrorist entities raise, collect and transfer funds all over the world to finance their attacks and support their day-to-day operations. They make use of everything from the formal banking system to money service businesses, to the physical transfer of gold.

Funds are vital to these organizations – and to the violence they perpetrate. It is therefore important that we deprive them of the money they need to plan and conduct their activities.

Canada's approach to cutting off funds to terrorist groups involves 11 departments and agencies. Additionally, financial service providers – such as banks – have an obligation to know their customers, keep records and report certain transactions to help identify money laundering and terrorist financing.

Law enforcement and intelligence agencies can use some of the information from these reports to assist in their efforts to identify and disrupt terrorist activities.

A challenge faced by Canada and other advanced nations is the pace of evolution within the financial sector. It can be difficult to keep up to date as financial technology advances and new platforms emerge that could be exploited for terrorist financing.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## INVESTIGATIVE CAPABILITIES IN A DIGITAL WORLD

We live in a digitized and highly networked world in which technological innovation is always forging ahead, advancing our quality of life, but also bringing new threats to our security.

The same technologies we enjoy and rely on everyday - smartphones, laptops and the like - can also be exploited by terrorists and other criminals to coordinate, finance and carry out their attacks or criminal activities.

We treasure our privacy, and rightly so, but we also expect law enforcement and national security investigators to be as effective in keeping us safe and secure in the digital world as they are in the physical world.

But our laws on how information can be properly collected and then used in court as evidence were mostly written before the rapid pace of new technology became a consideration. In the face of evolving threats, investigators worry about four main problems:

- slow and inconsistent access to basic subscriber information to help identify who was using a particular communications service at a particular time;
- the lack of a general requirement that domestic telecommunications networks maintain the technical ability to intercept messages;
- the use of advanced encryption techniques that can render messages unreadable; and
- unreliable and inconsistent retention of communications data.

Let's look at each of these challenges in turn:

### Basic Subscriber Information

Like looking up an address in a phone book or checking out a license-plate number, access to basic subscriber information is one way for law enforcement and national security investigators to identify an individual. But Canadian court rulings have reinforced the need for appropriate safeguards around basic subscriber information, some of which could, when linked to other information, reveal intimate details of a person's activities. These rulings, combined with the absence of a clear law governing access to basic subscriber information, have made it difficult for law enforcement to obtain it in a timely and effective manner. Some other countries allow police and intelligence agencies to obtain basic subscriber information without going to court.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## **Intercept Capability**

With legal authorization, the ability to intercept communications is a valuable tool in national security and criminal investigations. However, some communications providers are unable to comply with court orders to cooperate because they do not maintain the technical capability to do so. Their resulting inability to intercept communications can cause key intelligence and evidence to be missed.

## **Encryption**

Encryption technology is a tool that can be used to avoid detection, investigation and prosecution. After investigators get the proper legal authorizations and make a successful interception or seizure, the information obtained may be indecipherable due to encryption. And there is currently no legal procedure designed to require a person or an organization to decrypt their material.

## **Data Retention**

"Data retention" means the storage of telecommunications information - keeping track of which telephone numbers a person dials, for example, or how long calls last. Phone and Internet records of this kind can be critical to effective investigations. But there is no general requirement for communications providers to retain this information. Some delete it almost immediately. Some use it for their own commercial purposes, and then destroy it.

These and other challenges are amplified by the fact that data moves instantaneously across national boundaries. Communications providers may offer their services in Canada, but may have no business presence here, and thus operate beyond the reach of Canadian law.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## INTELLIGENCE AND EVIDENCE

We all want to ensure that Canada's national security information is protected. Indeed, the Government has an obligation to protect sensitive sources, capabilities and techniques. At the same time, there are instances in which this information may be required for a legal proceeding.

There are existing frameworks that govern the protection and use of national security information in a range of legal proceedings. For the most part, a Federal Court judge must decide whether disclosure of the information would hurt our international relations, national security or national defence. If so, the judge must then consider whether the public interest in disclosing the information outweighs the public interest in keeping it protected.

Sometimes, this means that a criminal court may be unable to hear the national security information – and may need to rely on an unclassified summary instead. Or it could be the case that, in a civil proceeding, a plaintiff may not have full access to the information required to make their case – or a defendant may be unable to mount a full defence. This raises the question of whether justice can truly be served in these examples.

There are also implications relating to immigration proceedings, where classified information is sometimes used. A good example is what is known as a “security certificate proceeding,” in which the Government makes the case that a non-citizen is inadmissible to Canada for reasons of security, violation of human or international rights, serious criminality or organized criminality.

In this case, a Federal Court judge rules on whether the certificate is reasonable. Former Bill C-51 made changes to immigration proceedings relying on classified information to better shield that type of information.

*This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.*

## CONCLUSION

We invite all Canadians to consider the questions raised in this Green Paper – and to read the longer and more comprehensive background document, which includes greater detail and a number of scenarios that help to illustrate what is at stake as we work to improve our security and intelligence framework.

Most of all, we encourage Canadians to let their opinions, ideas and potential solutions be heard.

As a starting point, here are a few questions to consider:

1. What steps should the Government take to strengthen the accountability of Canada's national security institutions?
2. Preventing radicalization to violence helps keep our communities safe. Are there particular prevention efforts that the Government should pursue?
3. In an era in which the terrorist threat is evolving, does the Government have what it needs to protect Canadians' safety while safeguarding rights and freedoms?
4. Do you have additional ideas or comments on the topics raised in this Green Paper and in the background document?

These are just suggestions to begin the dialogue as we seek the broad and meaningful contributions of Canadians.

Invariably, views will differ. Not all of us will share the same perspective on what is justified and what is reasonable. There will be strong opinions on which tools should be made available to the Government and its security and intelligence agencies, and which should not.

But that is what we want. We want to hear your views, and the views of your fellow Canadians.

Be mindful of our two-fold objective:

- To be effective in keeping Canadians safe;
- To safeguard our values, our rights and freedoms, and the open, inclusive and democratic character of our country.

We want to carefully consider the results of the consultations as we work to make meaningful improvements to Canada's national security laws and procedures.

**Respond to the Consultation Questions Online at**

**[Canada.ca/national-security-consultation](http://Canada.ca/national-security-consultation).**



other DPAs including our own Office, to develop a video featuring their Commissioner which would be released on Data Privacy Day. They chose not to participate, citing the potential of a perceived conflict of interest.

Both the UK and Australia told us their Facebook Pages have been effective outreach tools to connect with citizens and share information. Both have devoted some resources to ensuring they are creating original content for their Facebook Page. The UK ICO, for example, has created a number of short videos for their Facebook Page. The OAIC also shares relevant Facebook content posted by other Australian government agencies.

### ***Risk assessment***

Policy's risk assessment of the use of Facebook for outreach purposes identified three potential risks.

First, there is a reputational risk that an imposter Facebook Page could be created in the absence of an official Page created by our Office. Facebook has a mechanism for reporting fraudulent Pages, and to date, no imposter accounts for our Office have been found on Facebook.

Second, there is a risk that the Office could receive a Page-related complaint. Policy has assessed this risk and found that it is unlikely our Office would receive a complaint related to the Page feature. Additionally, Facebook Pages and their use as a tool for promoting brands and organizations are well-known to Facebook users. Policy has concluded that there is minimal risk that the OPC might be seen to be endorsing a non-privacy compliant Facebook feature. As noted above, our consultations have indicated that the UK ICO and the Office of Australian Information Commissioner also concluded that there was minimal risk that their respective organizations might be seen to be endorsing a non-privacy compliant Facebook feature through their use of a Facebook Page.

Finally, there is a risk that visitors to our Facebook Page could post personal information (either their own or the PI of someone else) on our Page. To mitigate this risk, Policy has recommended that we review all comments made to our Page before posting. Facebook Pages have the functionality to allow Page administrators to do this. We employ this same practice for comments readers make on our blog.

### ***Advantages of establishing a Facebook Page***

By establishing a Facebook Page, our Office would have an additional social media channel with which to communicate to individuals.

Research suggests that Canadians are avid social media users, with Facebook as the most popular social network among Canadians. A Forum Research survey conducted in 2015 found that 59% of respondents had Facebook accounts, compared to 30% of Canadian respondents on LinkedIn, 25% on Twitter and 16% on Instagram. (According to Facebook's own research, 14 million Canadians check their Facebook newsfeed every day.) Additionally, a study by the U.S.-based Pew Research Center study suggests that a large number of parents (66%) find parenting advice while looking at social media content.

## **Recommendation**

We recommend that the Communications Branch work toward establishing a Facebook Page.

We recommend that the Page be devoted to and focused on communicating to Canadians in general, as well as in connection with our youth and seniors outreach strategies.

We would use it to share existing and new OPC resources developed for individuals; inform the public of relevant news and announcements from our office; and share relevant Facebook posts from other DPAs and other federal government organizations (e.g. Public Safety's Get Cyber Safe Facebook Page and Innovation, Science and Economic Development's Your Money Matters Facebook page). An OPC Facebook Page would complement our current social media activity on Twitter, as well as our broader outreach efforts to the general public, and youth and seniors more specifically.

At the moment, small businesses would not be viewed as the primary target audience for use of this tool as small businesses tend to use the Facebook platform to reach customers (as opposed to using the platform as a source for information about running a business). In the future, we could decide to broaden our use of Facebook to reach small businesses as well.

The first step would be to develop a strategy outlining how the OPC intends to use Facebook. The strategy would outline the main objectives for the creation of a Facebook presence for our office – namely, that we would use it to communicate privacy-related information and advice to the general public, and in particular, to specific target groups within the general population (youth and seniors, as identified in our outreach strategies). It would outline how content for the Page would be developed and approved, and it would cover privacy-related matters (for example, we do not record or retain data about the Facebook users who follow us; and outline our rules of online engagement with the public).

We would consult with LSPRTA and the Office's CPO on the development of this strategy.

The strategy would also detail how we plan to launch the page – for example, informing other privacy commissioners' offices (within Canada and internationally) as well as other federal government departments managing Facebook Pages so that they may "Like" our Page and share our content with their followers.

The Communications Branch is currently in the process of staffing an IS-04 position and this resource would provide support for this initiative.

Should you agree with this recommendation, we would develop a social media strategy for Facebook and submit it to you for your approval before implementation.



**Revisions and/or approval**

- I approve this recommendation.
- I approve the recommendation with revisions noted.
- I have questions/concerns regarding this file and wish to discuss.

Comments :

Signature :