Plunkett, Shawn

From: Chayer, Marie-Helene
Sent: September-18-12 8:35 AM
To: Kwavnick, Andrea; Plunkett, Shawn
Subject: FW: [redacted]
Attachments: [redacted]

Thanks Andrea.

Shawn, over to you...

s.13(1)(c)
s.14(a)
s.15(1) - Subv

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – Politique sur les technologies d'enquêtes et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

From: Kwavnick, Andrea
Sent: September-18-12 8:34 AM
To: Chayer, Marie-Helene
Subject: FW: [redacted]

Bonjour Marie-Hélène,

[redacted]

I'm not sure who is taking on this file, so sending to you.

Thanks
Andrea

From: Audcent, Karen [mailto:Karen.Audcent@justice.gc.ca]
Sent: September-17-12 12:50 PM
To: Hatfield, Adam; Alex Beaulieu; Alter, Susan (RCMP) (Susan.Alter@rcmp-grc.gc.ca); Green, Amanda; André Carrier; Andre Leduc; Kwavnick, Andrea; Andy Kaplan-Myrth; Angers, Lucie (LANGERS@JUSTICE.GC.CA); Audcent, Karen; Bartlett, William (WBartlet@justice.gc.ca); Beata Nowakowska; Belanger, Pierre-Gilles (pbelange@JUSTICE.GC.CA); bernard.tremblay@rcmp-grc.gc.ca; Betty Ann Pottruff; Beverley Klatt; Blair Staples; Blanchette, François; Brews, Albert (abrews@justice.gc.ca); Cameron Gunn; Carole.Matthews@ontario.ca; Cathy Cooper; [redacted]; Chartier, Isabelle (ichartie@justice.gc.ca); Clement, Corrina (CClement@justice.gc.ca); Cloutier, Marie; Lapointe-Lavictoire, Colleen; Dale Tesarowski; Dan.Rajsic@ontario.ca; Dan Coté; Dan MacRury; Dave Black; [redacted] David Greening; Earl Fruchtman; einbinder-miller.rhona@cb-bc.gc.ca; eric.slinn@rcmp-grc.gc.ca; Deborah.Flak@ppsc-sppc.gc.ca; Francis Brabant; Frank Goldschmidt; Frederick Gaudreau; paul.gavrel@ec.gc.ca; Glen Lewis; Kousha, Hasti; Holthuis, Annemieke (AHOLTHUI@JUSTICE.GC.CA); Il Kim; Nancy.Irving@ppsc-sppc.gc.ca; Jacquie Nelson; Jamie.Prosser@ontario.ca; Jeff Beaulac; Moshonas, Jennifer; Jim Hughes; John Bilinski; John Turner; Josh.Hawkes@gov.ab.ca; Thompson, Julie; Kathy Collins; Kirk, Gordon (gkirk@justice.gc.ca); Laura Pitcairn; Lee Kirkpatrick; Lorraine Prefontaine; Lynne Kohm; Madgin, Philippe (pmadgin@justice.gc.ca); marc.moreau@rcmp-grc.gc.ca; mark.flynn@rcmp-grc.gc.ca; martin.charette@surete.qc.ca; McCann, France (FMCCANN@JUSTICE.GC.CA); Michael Bernstein; Mike Thompson; Nadine Nesbitt; Nguyen, Trang Dai (TNguyen@JUSTICE.GC.CA); Noël, Jean-François; Phyllis Harris; Pierre Piche; Rachel Melnychuk; Racine, Rose-Marie (RRacine@justice.gc.ca); Ram, Christopher; Renée Madore; Roni Pagliuso; Sansom, Gareth (GSansom@JUSTICE.GC.CA); Sarah Tanguay; Sebastien Bergeron-Guyard; Sergio Pasin; Sherri Lee; Shogilev, Matthew (MShogile@justice.gc.ca);

Susan Kennedy; Sylvain Fiset; Goguen, Taunya; Taylor, Matthew; Tom.Pownall@rcmp-grc.gc.ca; Tom Steenvoorden; Tony Pickett; Wayne Jacquard; William Beiersdorfer; Wong, Normand (NWONG@JUSTICE.GC.CA); Yves.Desjardins@rcmp-grc.gc.ca
Subject:

Hope everyone had a good summer.

Karen

J'espère que tout le monde a passé un bel été.

Karen

s.13(1)(c)
s.14(a)

Pages 3 to / à 5

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(c), 14(a), 16(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 6 to / à 8

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(c), 14(a)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 9 to / à 12

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(c), 14(a), 16(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 13 to / à 15

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(c), 14(a)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 16 to / à 17

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(c), 14(a), 16(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

FOR INTERNAL USE ONLY

Bill C-30 Enforcement Regime

- C-30's enforcement regime is a derivative of a standard enforcement regime that is found in over 100 Canadian statutes.

- The Bill includes two types of contraventions: violations and offences. Violations are punishable by administrative monetary penalties (AMPs) and would be issued by Public Safety Canada enforcement officials. Offences, on the other hand, are punishable by fines and would be levied by the courts.
    - Most contraventions of the Act can be proceeded against as either a violation or an offence, and the Bill gives discretion to PS enforcement officials to decide how to proceed.
    - Generally, contraventions that are more serious will be pursued as offences, while unintentional or less serious contravention will be pursued as violations.

- The Bill establishes different AMP and fine ranges depending on if the offender is an individual or a corporation.
    - For an individual, AMPs range from up to $25,000 for some contraventions, to up to $50,000 for others, and fines from up to $15,000 for some contraventions, to up to $250,000 for others.
    - For a corporation, AMPs range from up to $125,000 for some contraventions, to up to $250,000 for others, and fines from up to $15,000 for some contraventions, to up to $500,000 for others.

- An AMP or fine can be levied at the maximum amount for each day of contravention, e.g. $500,000 for 5 days equals $2,500,000.

- Corporate and director liability provisions exist.
    - If a contravention is committed, the Bill permits the employee that committed the contravention and the TSP to be held liable.
    - Corporate directors may also be held liable if they directed, authorized, assented to, acquiesced in or participated in the commission of the violation or the offence.
    - Due diligence provisions (i.e. the party did all he/she could to prevent the commission of the offence) exist.

- The Minister of Public Safety also has the option to seek a court injunction to stop a TSP from installing a particular piece of equipment that the Minister believes does not satisfy the requirements of the Act (.

s.21(1)(a)

Page 19

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(c), 14(a), 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

CURRENT STATUS

Bill C-30, the *Protecting Children from Internet Predators Act*, provides the power to make data preservation demands and orders. It does not, however, include provisions on data retention.

[redacted]

Original approved by:
Lynda Clairmont
Senior Assistant Deputy Minister
National Security

s.13(1)(c)
s.14(a)
s.21(1)(a)

RESPONSE TO PETITION
RÉPONSE À LA PÉTITION

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

PETITION NO./Nº DE LA PÉTITION	BY / DE	DATE
411-1784	Ms. May (Saanich—Gulf Islands)	September 24, 2012

RESPONSE BY THE MINISTER OF PUBLIC SAFETY
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

The Honourable Vic Toews

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

SUBJECT / OBJET
Telecommunications

RESPONSE / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL [X] TRANSLATION / TRADUCTION [ ]

Public Safety Canada

Canadians are concerned about crime, particularly crime involving children.

Reported child pornography offences were up 36% in 2010 in Canada (Statistics Canada, Police-reported crime statistics in Canada, 2010).

Inspector Scott Naylor, manager of the Ontario Provincial Police child exploitation unit, said that our current system for obtaining Internet Protocol (IP) addresses of suspected child pornographers isn't effective. "It's still like putting a cup under Niagara Falls. That's all we are catching".

That is why our Government introduced Bill C-30, the *Protecting Children from Internet Predators Act,* on February 14, 2012. The Government is now thoroughly reviewing this legislation.

Bill C-30 would not create new powers to access the content of e-mails or phone calls beyond that which already exists in Canadian law.

At all times we will strike an appropriate balance between protecting privacy and giving police the tools they need to do their job.

Today, telecommunications service providers (TSP) may provide authorities, without a warrant, with basic subscriber information under the *Personal Information Protection and Electronic Documents Act*. The problem is that there is no consistency across the country in how service providers respond to these requests: sometimes they respond in a timely manner, but often they respond only after considerable delays, if at all.

Specifically:

I. According to the Royal Canadian Mounted Police's (RCMP) National Child Exploitation Coordination Centre in Ottawa, in 2010, the average response time for a basic subscriber information (BSI) request was 13 days, and only 72.5% of requests were fulfilled.

II. One TSP only responds to BSI requests on Fridays, regardless of when the requests are submitted.

III. Another TSP only accepts BSI requests via email, which can be problematic in emergencies.

IV. In December 2010, New Brunswick RCMP began to investigate the distribution of child pornography. Police suspected an individual who was using a TSP who had historically not shared information with police. As a result, local police applied for a court order. There was a substantial delay and by this time the case had gone cold as the suspect had stopped his activities. Due to this delay, abuse could have been prevented at an earlier date as it was later discovered that this suspect was abusing two young boys to create child pornography. Several months later, the suspect resumed his online activity. This time the TSP was cooperative with police requests. The suspect was charged with possession and distribution of child pornography.

V. In 2007, the RCMP assisted with an international investigation in which suspects located in Canada were attempting to defraud American corporations of approximately $100 million. The investigation required police to find the individuals who were committing these fraudulent activities. The suspects were constantly on the move and police needed the immediate support of the TSPs to determine the location of these networks. However, the service providers would not provide police with the basic subscriber information they needed. Because of the lack of cooperation from the TSPs, it took eight full-time technical investigators five days to finally locate and arrest the suspects. The suspects successfully defrauded victims of $15 million. Had police been provided the information when it was requested, the value of the fraud would have been reduced considerably and police resources would have been used more effectively.

VI. A child was abducted in British Columbia in 2011. An amber alert was broadcast and, fortunately, the suspect returned the child. However, the suspect was not apprehended and his location remained unknown. Through further investigation, police obtained an IP address associated with the suspect. Police contacted the TSP directly and were advised that it was against policy to provide subscriber information related to an IP address without a Production Order. Police advised the TSP that the suspect had already abducted one child and that other children could possibly be at risk. The TSP decided to provide the information and the suspect was located and apprehended less than 24 hours after police received the information.

RESPONSE TO PETITION
RÉPONSE À LA PÉTITION

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

PETITION NO./Nº DE LA PÉTITION	BY / DE	DATE
411-1784	Mme May (Saanich—Gulf Islands)	24 septembre 2012

RESPONSE BY THE MINISTER OF PUBLIC SAFETY
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

L'honorable Vic Toews

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

SUBJECT / OBJET
Télécommunications

RESPONSE / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL [ ]
TRANSLATION / TRADUCTION [X]

Sécurité publique Canada

Les Canadiens sont préoccupés par le crime, particulièrement lorsque cela implique des enfants.

Les infractions de pornographie juvéniles déclarées par la police ont augmentées de 36% en 2010. (Statistiques Canada, Statistiques sur les crimes déclarés par la police au Canada, 2010)

L'inspecteur Scott Naylor, gestionnaire de la Section de la pornographie juvénile à la Police provinciale de l'Ontario, affirme que notre système pour obtenir les adresses protocole Internet (IP) des pornographes juvéniles présumés est inefficace. « C'est comme mettre une tasse sous les chutes Niagara. C'est tout ce qui est pris. »

C'est pourquoi nous avons introduit le projet de loi C-30, la *Loi sur la protection des enfants contre les cyberprédateurs*, le 14 février 2012. Le gouvernement examine présentement en détail ce projet de loi.

Le projet de loi C-30 ne créerait aucun nouveau pouvoir d'accéder au contenu des courriels ou à des appels téléphoniques qui iraient au-delà des pouvoirs qui existent déjà dans la loi canadienne.

En tout temps, nous atteindrons un juste équilibre entre la protection de la vie privée et le besoin de fournir aux policiers les outils dont ils ont besoin pour faire leur travail.

En vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, les télécommunicateurs peuvent, sans qu'un mandat soit nécessaire, transmettre aux autorités des renseignements de base sur les abonnés. Or, le problème est qu'il n'y a aucune uniformité à l'échelle du pays dans la façon dont les télécommunicateurs répondent à ces demandes. Parfois, ils y donnent suite rapidement, mais parfois, ils y répondent qu'après un long délai ou n'y répondent pas du tout.

Ainsi :

I. En 2010, selon le Centre national de coordination contre l'exploitation des enfants de la Gendarmerie royale du Canada (GRC) d'Ottawa, le temps de réponse moyen à une demande de renseignements de base sur les abonnés était de 13 jours et seulement 72,5% des demandent ont été exécuté.

II. Un certain télécommunicateur répond seulement le vendredi aux demandes de renseignements de base sur les abonnés, et ce, peu importe le moment où la requête est soumise.

III. Un autre télécommunicateur accepte seulement les demandes de renseignements de base sur les abonnés soumises par courrier électronique. Il va sans dire que cela peut s'avérer problématique lors de situations d'urgence.

IV. En décembre 2010, la GRC du Nouveau-Brunswick a commencé à enquêter sur un cas de distribution de pornographie juvénile. Les policiers soupçonnaient un individu qui utilisait un télécommunicateur reconnu pour ne pas fournir l'information demandée aux policiers. Sachant cela, le policier local a fait une demande d'autorisation. En raison de ce délai, des abus envers des personnes mineures n'ont pas pu être prévenus plus rapidement. De fait, il s'est avéré que ce suspect abusait de deux jeunes garçons afin de produire de la pornographie juvénile. Cependant, le suspect a arrêté ses activités en ligne durant la période d'obtention du mandat et l'enquête a été suspendue. Quelques mois plus tard, le suspect a repris ses activités en ligne et, cette fois, le télécommunicateur a accepté de fournir les renseignements demandés. Le suspect a été accusé de possession et de distribution de pornographie juvénile.

V. En 2007, la GRC a pris part à une enquête internationale visant des suspects qui se trouvaient au Canada et qui essayaient d'obtenir frauduleusement environ 100 millions de dollars de sociétés américaines. Au cours de l'enquête, les policiers devaient identifier les personnes commettant ces activités frauduleuses. Les suspects se déplaçaient constamment et les policiers avaient besoin de l'aide immédiate des télécommunicateurs pour déterminer où se trouvaient les réseaux. Cependant, les télécommunicateurs refusaient de fournir les renseignements de base sur les abonnés nécessaires. En raison du manque de collaboration des télécommunicateurs, il a fallu cinq jours à huit enquêteurs spécialisés travaillant à temps plein pour enfin trouver et arrêter les suspects, qui avaient alors déjà escroqué 15 millions de dollars à leurs victimes. Si les policiers avaient obtenu les renseignements dont ils avaient besoin lorsqu'ils les ont demandés, on aurait pu limiter considérablement le montant de la fraude et les ressources policières auraient pu être utilisées plus efficacement.

VI. Un enfant a été enlevé en Colombie-Britannique en 2011. Une alerte Amber a été diffusée et, heureusement, le suspect a libéré l'enfant. Toutefois, le suspect n'a pas alors été appréhendé, et on ignorait où il se trouvait. En effectuant une enquête plus approfondie, les policiers ont obtenu une adresse IP associée au suspect. Ils ont donc communiqué directement avec le télécommunicateur, et on leur a répondu que, sans une ordonnance de communication, il était contraire à leur politique de fournir des renseignements sur les abonnés liés à une adresse IP. Les policiers ont avisé le télécommunicateur que le suspect avait déjà enlevé un enfant et que d'autres enfants pourraient être à risque. Le télécommunicateur a alors accepté de fournir les renseignements demandés, et le suspect a été localisé et appréhendé moins de 24 heures après que les policiers ont obtenu les renseignements.

QUESTION PERIOD NOTE

Date: October 2012
Classification: UNCLASSIFIED
Branch / Agency: NS/Public Safety

Question Period Note

Bill C-30: *Protecting Children from Internet Predators Act*

ISSUE: Information respecting provisions contained in the "Lawful Access" bill, Bill C-30: *Protecting Children from Internet Predators Act*.

BACKGROUND:

The ability to intercept communications is a necessary tool for law enforcement and national security agencies to fulfill their mandates to support investigative and intelligence gathering activities. Powers to intercept communications are provided for in existing legislation, such as the *Criminal Code of Canada* and the *Canadian Security Intelligence Service Act*.

However, there is no statutory requirement for telecommunications service providers (TSPs) to make their networks intercept capable. As a result, authorities are often unable to intercept despite being lawfully authorized to do so. Bill C-30 would require TSPs to develop, implement and maintain a technical capability to enable lawfully authorized interceptions.

A second component of the proposed legislation is a requirement for TSPs to provide designated police, CSIS and Competition Bureau officials with basic subscriber information upon request. In specific emergency situations, TSPs could also be required to provide basic subscriber information to any police officer. Currently, the *Personal Information Protection and Electronic Documents Act* allows, but does not compel, TSPs to share this information with authorities. While some TSPs do so on a voluntary basis, others do not.

The legislation would also amend parts of the *Criminal Code*, the *Competition Act*, and the *Mutual Legal Assistance in Criminal Matters Act* in order to streamline the warrant application process for multiple investigative techniques (e.g. tracking) related to a single investigation that involves interception; introduce new safeguards for the existing use of warrantless interception powers conducted in exceptional circumstances; and, modernize some offences and investigative powers, including production orders and warrants for tracking and number recorders.

These amendments would provide Canada with the legal framework for ratification of the Council of Europe's *Convention on Cybercrime, and the Additional Protocol to the Convention of cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. They would also help to ensure that Canadian authorities have the tools they need to properly investigate modern crimes at the domestic level in an advanced telecommunications environment.

While developing the Lawful Access legislation, the Government carefully considered input from a broad range of stakeholders, including the telecommunications industry, civil liberties groups, victims and privacy advocates, police associations and provincial/territorial justice officials. Consultations were held in 2002, 2005 and 2007. The 2007 consultations, which were held in collaboration with Industry Canada, focused specifically on the subject of basic subscriber information.

Lawful Access legislation has been introduced in Parliament on a number of occasions. Bill C-30 combines elements of former Bills C-50 (*Improving Access to Investigative Tools for Serious Crimes Act*), C-51 (*Investigative Powers for the 21st Century Act*), and C-52 (*Investigating and Preventing Criminal Electronic Communications Act*), which were introduced in November 2010 and died on the Order Paper when Parliament was dissolved in March 2011. Earlier attempts were made in 2005 (Bill C-74, *Modernization of Investigative Techniques Act*) and 2009 (Bill C-47, *Technical Assistance for Law Enforcement Agencies Act*), but never advanced past First Reading.

LAWFUL ACCESS / L'ACCÈS LÉGAL

PROPOSED RESPONSE:

- **Today, when authorities are lawfully authorized to intercept an individual's communications, they are sometimes unable to do so because of a lack of technical capability on the part of the service provider.**

- **Bill C-30 would require telecommunications companies to build and maintain equipment capable of conducting these court authorized interceptions.**

- **It would also require telecommunications service providers to provide basic subscriber information to designated authorities upon request. This would not allow authorities to access the contents of an individual's emails, phone records or internet browsing activity without a warrant.**

- **The legislation would not compromise the privacy rights of Canadians. It would put in place specific privacy safeguards that do not exist today.**

- **This legislation is about giving authorities the tools they need to do their jobs in today's environment. It strikes the right balance between ensuring Canadians' security and protecting their privacy. It ensures that authorities can perform their jobs more efficiently, while maintaining a required level of accountability and transparency, giving them an investigative tool kit that is tailored to modern technology.**

CONTACTS:			
Prepared by Marcie Scott	Tel. no. Office: (613) 949-5886 BB: [redacted]	Approved by: Lynda Clairmont Senior Assistant Deputy Minister National Security **DRAFT - NOT APPROVED**	Tel. no. Office: (613) 990-4976 BB: [redacted]

Page 27

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(c), 14(a)

of the Access to Information

de la Loi sur l'accès à l'information

Page 28

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(c), 14(a), 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 29 to / à 30

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(c), 14(a)

of the Access to Information

de la Loi sur l'accès à l'information

Page 31

is withheld pursuant to section

est retenue en vertu de l'article

14(a)

of the Access to Information

de la Loi sur l'accès à l'information

Page 32

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(c), 14(a)

of the Access to Information

de la Loi sur l'accès à l'information

RESPONSE TO PETITION
RÉPONSE À LA PÉTITION

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

PETITION NO./Nº DE LA PÉTITION	BY / DE	DATE

RESPONSE BY THE MINISTER OF PUBLIC SAFETY
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

The Honourable Vic Toews

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

SUBJECT / OBJET
Bill C-30

RESPONSE / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL [X]
TRANSLATION / TRADUCTION [ ]

Public Safety Canada

Canadians are concerned about crime. We want to strike an appropriate balance between protecting privacy and giving police the tools they need to do their job. Our Government is thoroughly reviewing this legislation. Bill C-30, the *Protecting Children from Internet Predators Act*, would not create new powers to access the content of e-mails or phone calls beyond those which already exist in Canadian law.

RESPONSE TO PETITION
RÉPONSE À LA PÉTITION

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

PETITION NO./Nº DE LA PÉTITION	BY / DE	DATE

RESPONSE BY THE MINISTER OF PUBLIC SAFETY
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

L'honorable Vic Toews

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

SUBJECT / OBJET
Projet de loi C-30

RESPONSE / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL [ ]
TRANSLATION / TRADUCTION [X]

Sécurité publique Canada

Les Canadiens sont préoccupés par le crime. Nous voulons atteindre un juste équilibre entre la protection de la vie privée et le besoin de fournir aux policiers les outils dont ils ont besoin pour faire leur travail. Notre gouvernement examine présentement en détail ce projet de loi. Le projet de loi C-30, *Loi sur la protection des enfants contre les cyberprédateurs*, ne créerait aucun nouveau pouvoir d'accéder au contenu des courriels ou à des appels téléphoniques qui iraient au-delà des pouvoirs qui existent déjà dans la loi canadienne.

Page 35

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(b), 16(1)(c), 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Page 36

is withheld pursuant to sections

est retenue en vertu des articles

20(1)(b), 20(1)(c), 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Bill C-30 – An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts

Overview

An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts (known under the short title *Protecting Children from Internet Predators Act*) is a comprehensive Bill that contains one new statute – the *Investigating and Preventing Criminal Electronic Communications Act* (IPCECA) – and amendments to the *Criminal Code*, the *Competition Act*, and the *Mutual Legal Assistance in Criminal Matters Act*. This Bill is a response to the growing complexity of telecommunications technologies that underpin modern life, which have outstripped the ability of authorities to keep pace and are exploited by criminals, terrorists, and other individuals or groups to hide their illegal activities. Earlier iterations of this Bill were introduced in 2005, 2009, and most recently in 2010 as former Bills C-50, C-51 and C-52. This Bill contains six principal components.

Intercept capability. Bill C-30 requires telecommunications service providers to build and maintain intercept capable networks, thereby ensuring that new technologies can support authorized interception. This will ensure law enforcement and CSIS receive intercepted communications requested under lawful authority. The Bill will not substantially affect the competitiveness of the Canadian telecommunications industry, nor unnecessarily impair the privacy of individuals. This is the first of two components of the new IPCECA statute.

Basic subscriber information. Bill C-30 provides the police, CSIS and the Competition Bureau with consistent and reliable access to basic subscriber information, which is often required at the early stages of investigations or to fulfill general policing duties. Under current privacy legislation, this information may be provided to authorities by telecommunications service providers without a warrant, on a voluntary basis. Some choose to provide it voluntarily, while others insist on a warrant, which results in inconsistent access and delays across the country. Under the new provision, limited numbers of designated police, CSIS and Competition Bureau officials may request any of the following basic identifiers: the subscriber's name, address, telephone number, e-mail address, Internet Protocol address, and local service provider identifier. The Bill introduces strict controls and protections for the release of basic subscriber information, including record-keeping and audits, which do not exist today. Basic subscriber information is the second component of the new IPCECA statute.

Streamlined court order application process. The Bill reduces delays and redundancies associated with applying for warrants or orders that are related to an application for interception by creating a single application process for both the interception authorization and any related warrants or orders. Currently, in some provinces, police have to apply for different warrants or orders related to an interception authorization – tracking, dialed number recorder, etc. – separately. Bill C-30 will allow police to apply to a single judge for all the warrants relating to the same interception investigation simultaneously. This will ensure that one judge has the full picture of the investigation. The Bill will also harmonize the timeframes and provide automatic sealing of all of the warrants and orders, as is provided for in the case of authorizations to intercept private communications. This will prevent access to and the disclosure of the documents relating to the investigation.

New safeguards for interception of private communications in exceptional circumstances. Bill C-30 improves the public accountability of the interception regime by introducing annual public reporting of interceptions made in exceptional circumstances under s.184.4 of the *Criminal Code*. The Bill also includes provisions to notify individuals whose communications have been intercepted under these same circumstances. These safeguards would match those already included in the *Criminal Code* for other types of interceptions.

Modernizing some investigative powers. The Bill amends substantive offences and procedural powers of the *Criminal Code* to better address cybercrime and updates the *Criminal Code* to enable it to respond to today's telecommunications reality. New production orders will be established to reflect modern technologies, including for obtaining transmission data. Additionally, a new data preservation power will allow police and courts to require telecommunications service providers to preserve computer data for specified periods. These powers do not allow the police to obtain the preserved data. In order to do so, the police must return to the telecommunications service provider with a judicial authorization to that effect.

Ratifying the Council of Europe *Convention on Cybercrime*. Canada signed the Council of Europe's *Convention on Cybercrime* – the only existing international treaty on cybercrime – and its *Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, in 2001 and 2005 respectively, but has yet to ratify it. The amendments proposed in this Bill will allow Canada to ratify this important Convention and improve international cooperation on cybercrime. This will allow Canada to play its part in tackling global cybercrime challenges.

The tools and safeguards proposed in Bill C-30 are essential for the investigation and prosecution of crimes such as child pornography, drug trafficking and terrorism. The Bill maintains oversight thresholds consistent with current requirements and in many cases privacy protections are strengthened. It strikes the right balance between providing authorities with the tools they need to fight crime in the 21st century, while at the same time protecting the fundamental rights of Canadians.

Simplifying Lawful Access – Bill – C-30 – Through the Lens of Law Enforcement

Introduction:

When law enforcement uses words such as electronic interception, intercept capable, electronic surveillance and combines such words with the most widely used forms of communications by society – Internet, cellulars, social media.....it understandably raises concerns of many Canadians. So much so that when Canada's Privacy Commissioner surveys Canadians and states "More than eight in 10 respondents (82 percent) opposed giving police and intelligence agencies the power to access e-mail records and other Internet usage data without a warrant from the courts" most of us in law enforcement would back such a statement. But let's be fair, this is not what governments and Canada's law enforcement leaders are proposing.

These same technologies are providing a safe haven for serious criminal activity in Canada – organized crime, sexual predators, gangs, identity theft and terrorism are among the many examples. New technologies allow for old crimes to be committed in new ways, as well as new crimes to develop, including viruses, trojans, worms, hacking, spyware, spam, phishing, identity theft, Internet fraud and money laundering. The fact is that Canada's obsolete legislative scheme was implemented in 1975 during the days of the rotary dial telephone. Modernization of current legislative provisions is urgently required to reflect significant advancements in communications technologies. Without modernization, the current legislation severely challenges police investigations and compromises public safety. Urgent amendments are required to allow the police to lawfully and effectively investigate serious offences. This new law is up-dating laws to reflect new technologies.

We believe new legislation will:

- assist police with the necessary tools to investigate crimes while balancing, if not strengthening the privacy rights for Canadians through the addition of oversight not currently in place.
- help law enforcement investigate and apprehend those who are involved in criminal activity while using new technologies to avoid apprehension due to outdated laws and technology
- allow for timely and consistent access to basic information to assist in investigations of criminal activity and other police duties in serving the public (ie. suicide prevention, notifying next of kin, etc.)

One of the difficulties with regard to the lawful access legislation is presenting it in a fashion that the public can understand as it can be very technical. Our goal is to assist the public to allow them to base their opinion on fact, not rhetoric.

Today`s Environment versus the Proposed legislation:

Currently, there are few set procedures for law enforcement to gain information required to investigate leads relating to criminal activity. Telecommunication service providers (TSP`s) vary widely as to what information will be provided to law enforcement. The following table is used to describe the tightening of rules under Bill C-30 versus the current environment by various applications:

Application	Currently	Through Bill C-30
- Obtaining any content of email, cellular call, etc.	Obtainable only by way of warrant *	Obtainable only by way of warrant *
- Obtaining Basic Subscriber Information in the course of carrying out public safety activities	Ad hoc basis – some TSP's will provide, many others request warrant – Issue is timeliness and consistency in obtaining information – No controls exist on obtaining information	- strict limits on the number of law enforcement officials permitted to request information - those officials to be fully trained - strict procedures for recording, reporting and auditing of such requests - auditing/reporting process includes providing documentation to Minister of Public Safety, Privacy Commissioner, provincial authorities, etc.
- IP address or cellular tracking (monitoring)	- Could only be done through a warrant	- Could only be done through a warrant
- Monitoring Internet Surfing	- Could only be done through a warrant.	- Could only be done through a warrant
- Mechanism to obtain content of email, cellular call, etc.	Obtainable only by way of warrant * Ad hoc basis – TSP's are not required to preserve data. By time law enforcement obtains warrant, content may not be available. Severely handicaps law enforcement and may endangers lives	Obtainable only by way of warrant * - implements production and preservation orders.** - allows law enforcement to request TSP to preserve data while a warrant is being requested (helps ensure data is not lost)

* A warrant is a judicially authorized mechanism to allow law enforcement to gain private information (content or data). There are certain exigent circumstances (ie. life at immediate risk) where law enforcement can obtain this material. This does not change with Bill C-30.

** This legislation introduces production and preservation orders which police can present to a Telecommunication Service Provider. A production order would allow police to gain a limited amount of transmission data for the purpose of ultimately identifying the originating service

provider involved in the transmission of e-mails or other communications and would be granted through a warrant on the basis of "reasonable grounds to suspect." A preservation order request is one that requires the TSP to preserve (i.e. not delete) specific computer or communication data that would assist in an investigation for up to 21 days (90 days for foreign investigations) while police obtain a warrant to be able to view that data.

The Important Facts Around the Legislation:

Access to Actual Data or Content:

Fact: To gain content of electronic communications, a warrant is required. Data or content of transmissions can only be released to law enforcement through a court ordered warrant process. The legislation does not change this. (There are very limited exceptions to this in emergency situations where serious harm must be prevented).

The preservation of data (a 'demand' by a police agency) is a request to a service provider to preserve data for a time period not exceeding 21 days (in order that the police have the opportunity to apply for the requisite warrant to obtain the information). This will necessitate the securing of existing data by the provider and the housing of that data in anticipation of the warrant.

Fact: There is nothing in the bill that asks the provider to specifically monitor the traffic of the individual and report back to the law enforcement agency on the activity of an individual (i.e., this is not a "collection order").

Access to Basic Subscriber Information:

The information which companies would be compelled to release would be: name, address, phone number, email address, Internet protocol address, and the name of the service provider. All of these would involve police providing one identifying set (e.g., IP address and time/date) and the communication service provider providing the matching subscriber information (e.g., customer name). While this information is important to police in all types of investigations, it can be of critical in cases where it is urgent that police locate a caller or originator of information that reasonably causes the police to suspect that someone's safety is at risk. Without this information, the police may not be able to quickly locate and help the person who is in trouble or being victimized.

Fact: Gaining basic subscriber information (names, addresses, phone numbers etc.) would be obtainable pursuant to requests from designated officials in policing agencies through an audited process. This reflects the reality that phone directories do not necessarily exist in the digital world.

The Auditing Process:

Currently, there is no audited process for law enforcement to gain access to basic subscriber information. It may be obtained through a current relationship between a policing service and a TSP or, far too often, is only provided following significant delays. Some TSPs outright deny providing the information without a warrant. *Currently law enforcement agencies are not directly accountable for these requests and for the information that they obtain.*

Fact: Under the proposed legislation, new safeguards will be implemented which actually enhance the privacy of Canadians. These include:

- *strict limits on the number of law enforcement officials permitted to request information*
- *the training of such individuals*
- *strict procedures for recording, reporting and auditing of such requests*
- *the implementation of an auditing/reporting process which includes providing documentation to Public Safety Minsters, Privacy Commissioners, Federal and provincial authorities, etc.*

Compliance by telecoms and ISPs:

Intercepting communications has been cited as an issue because of the cost-prohibitive nature of these upgrades to existing service providers and new entrants into the market.

Fact: *Within this legislation the government recognizes the cost of development for the providers and is prepared to assist in specific circumstances. There is wording that speaks to grandfathering existing providers and the permission of a catch-up period with the possibility of government financial assistance.*

Other:

Tracking of Phones (which have GPS) in the absence of a warrant. Such a possibility currently exists within the Criminal Code (s.487.11), but only for an exigent circumstance (i.e. a kidnapping or extortion). This same section will remain (slightly revised to include a Number Recorder) in the new legislation.

Lawful Access Frequently Asked Questions

Q1

Why do police need warrantless access to basic subscriber information (i.e. subscriber name, address, the existence of services, account information)?

A1

- *Basic subscriber information is often the most basic piece of information needed to progress an investigation, which may later require obtaining a warrant. It is similar to connecting a person's name to their telephone number in an address book. Lack of timely access to such information can, and often does, block investigations. In the case of situation, such as reports of potential suicides, lives can be endangered.*

- *Currently, there are few set procedures for law enforcement to gain information required to investigate leads relating to criminal activity. Telecommunication service providers (TSP`s) vary widely as to what information will be provided to law enforcement. This new legislation will:*

    - *assist police with the necessary tools to investigate crimes while balancing privacy rights for Canadians*
    - *help law enforcement investigate and apprehend those who are involved in criminal activity while using new technologies and avoid apprehension due to outdated laws and technology*
    - *allow for timely and consistent access to basic information to assist in investigations of criminal activity*

- *Towards the end of this document, we have provided a section entitled: "Case Studies: The Utility of Basic Subscriber Information to Law Enforcement" as examples of why police need access to basic subscriber information. As an example of the issue, according to the RCMP's National Child Exploitation Coordination Centre, in 2010, the average response time for a basic subscriber information request was 12 days, and only 72.5% of requests were fulfilled*

- *Other applications:*

    - *Ascertain the address of a witness who has provided their phone number(s).*
    - *To follow up leads in an investigation where they have been provided a phone number and need to:*

- *know if it belongs to the person it is purported to belong.*
- *establish an address at which the person resides (presuming the number is a landline because address information on cellular phones is unreliable at best)*

- *To have the information required to obtain a warrant (customer name and address, IP address, phone number, etc.)*
- *As identified above, in emergent cases such as 9-1-1 calls from a cell phone or similar distress communication over the internet. This information may be essential to ensure help is provided to a person as soon as possible.*
- *To expedite investigations involving serious critical matters which require swift police response to apprehend criminals or prevent crime.*
- *To notify next of kin when there has been an accident or homicide*
- *To notify owner when stolen property is recovered.*

Q1 (A)

Why can't police just get a warrant for Basic Subscriber Information?

A1 (A)

- *It may not allow for timely response and potentially jeopardize lives and safety while warrant is being obtained. In many cases, time is of the essence.*
- *It may allow victimization to continue while police attempt to get the warrant*
- *In many cases, law enforcement cannot obtain a warrant without BSI.*
- *How does law enforcement get a warrant for possible suicide threats, next of kin notification on a timely basis?*
- *In the case of missing persons, police often do not have obvious grounds that a crime is involved, nor that it is urgent. A warrant is likely not obtainable, based on the information provided, and the Telecommunication Service Providers (TSP's) are not required to provide BSI . In these cases, the first 24 hours of an investigation is critical.*
- *BSI allows us to investigate expeditiously with minimal intrusion (contact information) into peoples lives*
- *If a warrant was required for each request, police (and Justices) could not keep up with the demand. Further, the complexity of cross-jurisdictional (provincial / national / international) would place a significant workload on policing to obtain warrant for BSI in each location.*
- *Please note: The notion of urgency can be somewhat subjective. With this legislation, it addresses the issue of a uniform policy to gaining such information.*
- *Again, in today's environment, TSP's may be willingly provide BSI information and they may not depending on the practices of individual TSP's. With this legislation, oversight is incorporated which is currently not in place. <u>Law Enforcement is seeking consistency and ensuring that the TSP's are not the ones who randomly decide what we can, or cannot, investigate.</u>*

Q2

Who can ask for basic subscriber information from service providers?

A2

Currently any sworn or civilian police personnel can request this information from a telecommunications company. The new legislation will require the head of a law enforcement agency (i.e. the Chief or Commissioner) to designate a limited number of people within the organization to obtain this information. Mandatory training will be required of all designated officials. Law enforcement will be required to document all requests and disclose them through an audit procedure contained within the bill. The audit procedure includes:

- *strict limits on the number of law enforcement officials permitted to request information*
- *the training of such individuals*
- *strict procedures for recording, reporting and auditing of such requests*
- *the implementation of an auditing/reporting process which includes providing documentation to Public Safety Minsters, Privacy Commissioners, Federal and provincial authorities, etc.*

Q3

What is done with the basic subscriber information obtained by law enforcement personnel from the service providers?

A3

This information is provided to police personnel to aid in investigations and for public safety purposes.

- *There is currently an accepted rule that the information obtained may only be used for the purpose for which it was obtained. There is no body which monitors this at the moment, and no requirement for law enforcement agencies to be accountable for why the information was obtained and how it was used.*

- *The new legislation ensures that:*

    - *law enforcement agencies can account for the reason the information is obtained and also what the information was used for.*
    - *the agency may only use the information for the purpose for which it was obtained.*
    - *the agency organize the information in a fashion that would permit an audit of that information to determine why it was requested and what the information was used for.*

Q4

Do law enforcement agencies actually engage in the interception of private communications without a warrant/judicially approval?

A4

Since 1993, Section 184.4 of the Code has provided that peace officers can intercept private communications without prior judicial authorization, where the peace officer believes on reasonable grounds that: (i) an authorization cannot be obtained with reasonable diligence, given the urgency of the situation; (ii) an interception is immediately necessary to prevent an unlawful act that would cause serious harm to any person or to property; and (iii) either the originator or the intended recipient of the private communication is the person who would perform the harmful act or is the intended victim.

In 2008 the constitutionality of this Section was questioned in a Court case R v. 6 Accused (There is a pending SCC decision). The legislation, as currently written lacks the requirement of reporting to the Attorney General (Provincial) or to Public Safety Canada (Federal) of the use of this measure. Additionally, unlike traditional judicially approved interception, it lacks the requirement of notification to the person(s) intercepted. The former Bill C-50 intended to amend the current legislation to ensure that both these deficits were rectified.

Q5

Will the new legislation actually empower Internet Service Providers (ISPs) to collect information and provide it to law enforcement agencies in the absence of a warrant?

A5

Absolutely not. The law enforcement agency will be permitted the ability to make a "demand" to preserve data for 21 days, which means that the data will be preserved for that time period by the service provider, but the law enforcement agency MUST have a warrant to obtain the data that was preserved by that demand (or to extend the preservation by judicial order for an additional 90 days).

Q6

Won't the new legislation cripple the telecommunications and internet service provider companies financially with all the new requirements to have intercept capability?

A6

This was considered in the drafting of the legislation. Within this legislation the government recognizes the cost of development for the providers and is prepared to assist in specific

circumstances. There is wording that speaks to grandfathering existing providers and the permission of a catch-up period with the possibility of government financial assistance. Note that much more far-reaching laws exist in the United States and Europe where TSP's, (based on competition) have not passed on costs to consumers.

Q7

For those of us who live our lives online and presume that there is some anonymity in that realm, doesn't this legislation provide "the state" the ability to watch our actions and collect information about us on a whim?

A7

This is absolutely not true. This legislation is not designed to do away with the need for a warrant for information currently obtained by way of warrant. This legislation is designed to bring the Criminal Code into this century and this decade and provide for the ability to preserve data that might not otherwise be retained, to allow for law enforcement agencies to apply for the warrants to obtain the information. Crimes involving the use of services and sites available on the internet are on the increase – from child exploitation to identity theft – and law enforcement agencies require the ability to obtain the data required to determine whether the person suspected has committed a crime. This information could only be obtained with the issuance of a warrant by a judge.

The basic subscriber information provision does not give law enforcement the lawful authority to monitor websites for the purpose of creating profiles of individuals, or to track individuals. Under this legislation, police may request the name and address associated with an IP address using a basic subscriber information request.

Requests for information from a telecommunications service provider about the website surfing activity or the real-time whereabouts of an individual would need to be made under production orders, warrants or wiretap authorizations contained in the Criminal Code.

Q8

I heard that telecommunications companies and ISPs will track my location through my phone or internet use and will provide this information to law enforcement. Is this true?

A8

Currently, and as well with the new legislation, such action can only take place with a warrant or in an exigent circumstance telecommunications companies and ISPs will provide this information to law enforcement agencies. A warrant will be required to obtain this information unless a law enforcement agency invokes either s. 487.11, s. 184.4, or s.492.1 of the Criminal Code. Where there have been changes, the new legislation puts new privacy and Charter protections in place and ensures that the service providers must have the capability to provide the information.

Q9

Isn't this legislation simply an attempt by the government and police to position "the state" to have eyes and ears everywhere and have the ability to invade personal privacy at a whim?

A9

The intent of the legislation is to compel service providers to have the capability to intercept private communications under judicial order or in an exigent circumstance. It also stipulates that tombstone information must be provided to law enforcement personal in the absence of a warrant (whereas there is no legislation dictating this or otherwise at the moment) but clarifies the rules that both the police and the service provider must follow. For example, because a service provider would be compelled to disclose, it now places an additional burden on the law enforcement community to provide a clear audit of what the information was requested for and how it was utilized once received (for which there is no current requirement).

Federal Ombudsman for Victims of Crime on the need for Lawful Access

The Office of the Federal Ombudsman for Victims of Crime is an arms-length resource for victims in Canada. The Office was created in 2007 to ensure the federal government meets its responsibilities to victims of crime. Ms. Sue O'Sullivan is Canada's Federal Ombudsman for Victims of Crime. Both her, and her predecessor's have documented the need for Lawful Access.

The Ombudsman has underlined the importance of the issue of child sexual exploitation and the need for lawful access to Parliament. In the report "Every Image, Every Child – Internet-Facilitated Child Sexual Abuse in Canada" the Ombudsman outlines the very serious issues faced by law enforcement. In her testimony before a Senate Standing Committee on Bill C-22 (An Act respecting the mandatory reporting of internet child pornography by persons who provide an internet service) she states:

> *While I am fully supportive of this bill, I must also point out that there is still much more to be done in order to effectively address the issue of Internet-facilitated child sexual abuse. Bill C-22 will not, in and of itself, eradicate child sexual abuse material from being created or shared; nor will it address the challenges that law enforcement will face in pursuing these cases without the necessary authority to compel ISPs to provide basic customer name and address information in order to identify and locate the individuals associated with a particular IP address.*
>
> *Currently in Canada, ISPs are allowed but not obliged to provide customer name and address information without a warrant. Though many companies do cooperate, some can and do refuse to cooperate with law enforcement. In fact, according to the National Child Exploitation Coordination Centre in 2007, 30 per cent to 40 per cent of requests are denied. Without this information, law enforcement may be forced to close a case before a detailed investigation ever begins.*
>
> *When it comes to privacy, the victim's privacy issues also need to take precedence. I do not think there is anything that violates your privacy more as a victim than having your sexual abuse be out there circulating in cyberspace. It is about balance and about respecting the privacy rights of the victims of sexual abuse*

For further information:

- Ms. O'Sullivan testimony February 10, 2011 before the Senate Standing Committee on Legal and Constitutional Affairs on Bill C-22: http://www.parl.gc.ca/Content/SEN/Committee/403/lega/20evb-e.htm?Language=E&Parl=40&Ses=3&comm_id=11
- Every Image, Every Child report: http://www.victimsfirst.gc.ca/res/pub/childp-pjuvenile/cont_01.html
- Every Image, Every Child backgrounder: http://www.victimsfirst.gc.ca/media/news-nouv/bg-di/20090507-1.html
- Every Image, Every Child fast facts/statistics document: http://www.victimsfirst.gc.ca/media/news-nouv/bg-di/20090507-2.html

Case Studies: The Utility of Basic Subscriber Information to Law Enforcement

One of the problems with the current system is that there is no uniformity or reliability as to how/if TSPs respond to requests for basic subscriber information. For instance:

- There is one TSP that only responds to BSI requests on Fridays, regardless of when the requests are submitted
- There is one TSP that only accepts BSI requests via email

The National Child Exploitation Coordination Centre in Ottawa looked at a sample of 1,244 of the basic subscriber information requests they made in 2010. TSPs provided the information in 902 cases (72.5%). However, in 62 cases (5%), the TSPs refused to provide the information without a court order and in 53 cases (4.3%) did not respond to the request. In 227 cases (18.2%) the TSPs did not have the information that authorities requested. These numbers do not include requests made by other units that investigate Internet child exploitation offences across the country.

Furthermore, in 2010, the average response time for these requests was 12 days.

The National Child Exploitation Coordination Centre in Ottawa reported that, in 2007, of the 482 requests they made for basic subscriber information, in 19 cases (3.9%) service providers refused to provide the information without a court order and in 92 cases (19.1%) they did not respond to the request. In 40 cases (8.3%) the service providers did not have the information that was requested. In 2008, the NCECC in Ottawa made 335 requests for basic subscriber information. In 6 cases (1.8%) service providers refused to provide the information without a court order. In 46 cases (13.7%) they did not respond to the request and in 30 cases (9%) the service providers did not have the information that was requested.

Examples of regional disparity regarding telecommunications service providers (TSPs) providing BSI

Sometimes TSPs in specific regions don't respond to requests. Some TSPs in Atlantic Canada will not provide BSI unless they have a warrant.

1) In December 2010, New Brunswick RCMP began to investigate a case of peer-to-peer sharing of child pornography. Police suspected that up to 170 IP addresses were associated with a single individual. These IP addresses belonged to a TSP known for refusing to voluntarily provide subscriber information without a court order so the police applied for one.

   As a result, the basic subscriber information was provided 15 days later and by that time the suspect's Internet activity had stopped. In September 2011, the suspect resumed his online activity and, that time, the TSP provided the basic subscriber information voluntarily. This cooperation allowed the police to act quickly and arrest the suspect at his residence in October 2011. The suspect was charged with possession and distribution of child pornography. Furthermore, police discovered that he was also producing child pornography and he was charged with that crime as well. The suspect also pled guilty to charges, which included the abuse of two young males from New Brunswick. If the police had been able to obtain the

information shortly after the investigation began, the investigation could have proceeded to the arrest stage more rapidly and the suspect's sexual abuse could have been stopped sooner.

Examples where TSPs did not provide police with BSI

2) In 2007, there was an international case involving 88 Canadian Internet Protocol addresses linked to the purchase of child pornography. The police requested the basic subscriber information associated with these addresses. Fifty one requests were answered and police were able to investigate these individuals and in some cases charges were laid. However, 37 requests were unanswered by the service providers. As a result, the identities and location of these suspected pedophiles is still unknown today.

3) In Operation Koala, a major international child pornography case in 2008, Europol provided the RCMP with information relating to 98 Canadian e-mail accounts or Internet Protocol addresses. TSPs were asked to provide the related basic subscriber information about their customers. Many service providers did provide the basic information and it led to the arrest and prosecution of nine Canadians. Regrettably, the identity of 25 Internet Protocol addresses or e-mail accounts could not be established due to the lack of cooperation of some service providers.

4) In Project Penalty, an international child pornography investigation, 47 out of 200 requests for basic subscriber information were refused by the TSPs.

5) In 2007, the RCMP assisted with an international investigation in which suspects located in Canada were attempting to defraud American corporations of approximately $100 million. The investigation required police to find the individuals who were accessing unsecured wireless computer networks in the Toronto area (war driving) to commit these fraudulent activities. The suspects were constantly on the move and police needed the immediate support of the TSPs to determine the location of these networks. However, the service providers would not provide police with the basic subscriber information they needed. Because of the lack of cooperation from the TSPs, it took eight full-time technical investigators five days to finally locate and arrest the suspects. The suspects successfully defrauded victims of $15 million. Had police been provided the information when it was requested, the value of the fraud would have been reduced considerably and police resources would have been used more effectively.

6) A 2006 international criminal investigation involved 78 Canadian Internet Protocol addresses linked to the purchase of child pornography. Requests for basic subscriber information related to those Internet Protocol addresses were submitted to the relevant TSPs and the information was provided for 44 addresses. However, 18 suspects have not been identified since the service providers refused to provide the basic subscriber information without authorities first obtaining a warrant.

7) In 2009, the RCMP in Alberta were notified of a threat made online to carry out a school shooting. Police had the Internet Protocol address and the date and time the threat was made and police requested that the TSP provide the corresponding basic subscriber information. The provider refused to cooperate, saying there was no urgency because the threat to carry out the shooting was six days old. The following day (Friday before a long weekend) police applied for a production order to compel the TSP to provide the information. By the time the production order was issued, the contact at the TSP had left for the weekend and the police had to wait three days before obtaining the information. When the TSP did provide the information, the

police used the information to obtain an additional warrant authorizing the search of a residence. A young person was arrested and remanded pending a mental health evaluation.

Examples of how BSI is useful to locate or identify an individual

8) In 2008, Calgary police were investigating threatening emails that were being sent to a woman from a sender whose identity was concealed. Authorities provided the TSP with the IP address and asked the TSP for the street address from where the emails were sent. The information was provided and, as a result, within one day police were able to identify the individual sending the threatening emails and the investigation was complete. The individual was charged with criminal harassment and the victim got a restraining order against this individual.

9) A child was abducted in British Columbia in 2011. An amber alert was broadcast and, fortunately, the suspect returned the child. However, the suspect was not apprehended and his location remained unknown. Through further investigation, police obtained an IP address associated with the suspect. Police contacted the TSP directly and were advised that it was against policy to provide subscriber information related to an IP address without a Production Order. Police advised the TSP that the suspect had already abducted one child and that other children could possibly be at risk. The TSP decided to provide the information and the suspect was located and apprehended less than 24 hours after police received the information.

10) In 2008, the head of a municipal government in Québec was receiving death threats and harassing calls. In this case, the TSP cooperated and provided basic subscriber information to the police when it was requested and the police were able to locate and arrest the suspect. When the suspect was arrested, the police seized weapons from his house.

11) The Toronto Police Services had at least two cases involving citizens calling the police to advise that they were communicating over the Internet with persons threatening suicide. In both cases, the location of the potential victims was unknown. The police contacted the hosts of the websites and were provided with the IP addresses associated with the suicide threats. The police then contacted the TSPs and were provided with the basic subscriber information without a court order. This allowed the police to locate the distressed persons before they could harm themselves.

Example of how BSI is useful in the early stages of an investigation

12) In 2009, police were called to a homicide in which the victim suffered multiple stab wounds and was left on the street. The police determined that the victim had been involved in an altercation after attending a local pub. One of the victim's friends told police that one of the men suspected of being involved in the murder had called the victim's cell phone prior to the murder. The police looked through the victim's phone and found the cell number of this suspect. The police then provided the suspect's cell phone number to a TSP and obtained the basic subscriber information associated with that number. As a result, the police were able to identify the suspect, and from there more suspects were identified. As information beyond basic subscriber information was required, the police applied for a production order and obtained incriminating text messages.

13) In 2009, a Calgary-based company with 15,000 employees had its server hacked. A large amount of corporate data was stolen including personal records and payroll information. During their investigation, police obtained an IP address from the company, identified the TSP and asked the TSP for the name and address of the customer associated with the address. The TSP refused to voluntarily provide basic subscriber information to the police, so the police obtained a search warrant and the information was provided five days later. The information allowed the police to obtain a search warrant in relation to a residence in Manitoba. Pursuant to the search warrant, police seized the computers of one of the company's previous employees, but the delay that occurred was harmful to the company as the information that was stolen was of great potential use to the company's competitors.

<u>Examples of the need for interception capability</u>

14) In 2008, members of an organized crime group in British Columbia were directing an Agent to commit criminal acts, such as extortion and drug trafficking, through messages on cellular telephones. The service provider did not have the capability to intercept these messages and it took the RCMP six weeks to devise and implement a technical solution. The inability of police to intercept the text messages at a critical point in the investigation meant vital evidence was not collected.

15) The RCMP had installed equipment at a service provider to support an international money laundering and drug investigation. When a separate international terrorism investigation got underway, the police had to redeploy the interception equipment from the money laundering investigation in order to intercept the communications of the primary terrorism target. As a result of having to redeploy the equipment, evidence was lost in the money laundering investigation. If interception capability obligations had been in place, both interceptions could have been performed and evidence would not have been lost.

The Canadian Association of Chiefs of Police has obtained many further examples of the utility of Basic Subscriber Information to Law Enforcement which will be provided in our release to Committee.

Canadian Association of Chiefs of Police / Association canadienne des chefs de police

300 Terry Fox Drive, Unit 100, Kanata, ON K2K 0E3
Tel./Tél. (613) 595-1101 - Fax/Téléc. (613) 383-0372 www.CACP.ca

MEDIA ADVISORY

FOR IMMEDIATE RELEASE

Canadian Association of Chiefs of Police Renew Appeal

"We Can't Stand By And Do Nothing!"

Vancouver, BC – On Friday, October 26, 2012, Chief Constable Jim Chu, President of the Canadian Association of Chiefs of Police (CACP) will be holding a national media conference on the issue of Lawful Access, currently in the form of Bill C-30 "Protecting Children from Internet Predators Act."

Chief Constable Chu and other participants will be available for interviews following the event.

Date / Time: Friday, October 26, 2012, 10:00 – 11:00 a.m. (Pacific Standard Time)

Location: First Floor Media Room: Vancouver Police Department 2120 Cambie St., Vancouver, B.C.

Please note that this press conference will be live streamed and can be viewed by going to the Vancouver Police Department website at vpd.ca and/or click on View VPD press conferences live.

For further information, please contact:

Constable Brian Montague
Media Relations Officer
Vancouver Police Department
Tel.: 604-717-2807 Email: brian.montague@vpd.ca

Timothy M. Smith
Government Relations and Strategic Communications
Canadian Association of Chiefs of Police
Tel.: 613-601-0692 Email: timsmith2000@rogers.com

The Canadian Association of Chiefs of Police (CACP) was established in 1905 and currently has greater than 1,000 members from all across Canada. Through its member police chiefs and other senior police executives the CACP represents in excess of 90% of the police community in Canada. Our members include federal, First Nations, provincial, regional and municipal, transportation and military police leaders. The mission of the CACP is "leading progressive change in policing

Canadian Association of Chiefs of Police / Association canadienne des chefs de police

300 Terry Fox Drive, Unit 100, Kanata, ON K2K 0E3
Tel./Tél. (613) 595-1101 - Fax/Téléc. (613) 383-0372 www.CACP.ca

MEDIA RELEASE

FOR IMMEDIATE RELEASE
October 26, 2012

Police Confirm Canadians' Top Five Fears About Lawful Access

CACP Renews Appeal for Lawful Access Legislation

VANCOUVER, BC – The Canadian Association of Chiefs of Police (CACP) is launching a renewed effort to inform Canadians as they debate police authority for 'lawful access', in the context of Bill C-30 – *"Protecting Children from Internet Predators Act."*

"If we stand by and do nothing, criminals will continue to exploit today's technologies to criminally harass and threaten others and commit frauds, scams and organized and violent crimes with little fear of being caught. Canadians need the same protection against criminals that other western democracies enjoy," stated CACP President Chief Constable Jim Chu.

Previous Canadian governments have introduced lawful access legislation only to have it 'die on the order paper.' The CACP is not willing to watch Bill C-30 fall victim to a similar fate.

"If we don't take a strong stance on this issue, Canadians will not appreciate the limitations that constrain law enforcement in the cyber world. Law enforcement continues to be handcuffed by legislation introduced in 1975, the days of the rotary phone. Today we allow new technologies to be used as a safe-haven for serious criminal activity, but are pulling back from using technology to prevent and investigate these serious crimes," Chu continues.

"If the laws from the 1970s are not modernized, then organized criminals will plan their killings and kidnappings using telecommunications providers who do not build into their systems the technical ability to be monitored for the purpose of gathering evidence. Terrorists will exploit these same gaps. Victims who have been scammed or extorted over the Internet will be told the electronic footprint linking the suspect to the crime has disappeared because the telecommunications provider has no legal obligation to preserve data. If a suspect lures a child using a landline phone, basic subscriber information is available in a phone directory. But predators today don't use old technology. The parent of a child who has been lured over the Internet will be told that the police search for their child is delayed because a warrant has to be obtained for basic subscriber information."

"Criminal bullying is extremely concerning to all Canadians, especially the parents of young children, and Bill C-30 also provides new legislation to help police intervene and investigate cyber bullying in their early stages to prevent needless tragedy. The Bill makes it an offence to use telecommunications, including social media and the internet, to injure, alarm and harass others. "

Canadians need to understand what lawful access is truly about.

The CACP has created a video entitled "Police Confirm Canadians' Top Five Fears About Lawful Access" which can be viewed at http://youtu.be/ymVqkugH8PU In addition, to promote informed discussion on this issue, the CACP has prepared a document entitled "Simplifying Lawful Access – Through the Lens of Law Enforcement." It is available on the CACP website (www.CACP.ca) or directly at http://www.cacp.ca/media/library/download/1243/Final_Simplifying_Lawful_Access_final_english.pdf

The document compares today's environment to the proposed new legislation, provides answers to 'frequently asked questions' and includes a series of case studies describing how law enforcement uses basic subscriber information.

While the CACP endorses Bill C-30, we would like to make it clear there is one part of the bill that has posed concerns to some and we share that concern. Section 34 is currently worded suggesting that an inspector can search anything, including a Canadian's private information at a telecommunications provider's facility, to verify compliance with the act. It is easy to understand why some might conclude from such wording that inspectors would have unfettered access to Canadians' personal records when doing these inspections. While we realize this is not the intention of this section, this must be clarified. We recognize such inspections are required but the wording in Section 34 needs to be changed to assure Canadians that their personal information will never be a part of that inspection."

The CACP urges our politicians to provide police with modern tools so they can better protect Canadians from harm. Bill C-30 would achieve this. The CACP agrees with the stronger accountability and oversight provisions in C-30 that protect the public against misuse of police intercept powers.

The CACP urges Members of Parliament, the media and all Canadians to review the importance of this legislation through the lens of today's victims of crime, and the frontline law enforcement officers who are trying to prevent and investigate crimes.

The Canadian Association of Chiefs of Police was established in 1905 and represents approximately 1,000 police leaders from across Canada. The Association is dedicated to the support and promotion of efficient law enforcement and to the protection and security of the people of Canada. Through its member police chiefs and other senior police executives, the CACP represents in excess of 90% of the police community in Canada which include federal, First Nations, provincial, regional and municipal, transportation and military police leaders.

For further information, please contact:

Timothy M. Smith,
Government Relations & Communications
Canadian Association of Chiefs of Police
Tel.: 613-601-0692
Email: timsmith2000@rogers.com

2012-2013 Supplementary Estimates (B)

BILL C-30,
THE PROTECTING CHILDREN FROM INTERNET PREDATORS ACT

- **Canadians are concerned about crime. We want to strike an appropriate balance between protecting privacy and giving police the tools they need to do their job. Our Government is thoroughly reviewing this legislation. Bill C-30, the *Protecting Children from Internet Predators Act,* would not create new powers to access the content of e-mails or phone calls beyond those which already exists in Canadian law.**

QUESTIONS AND ANSWERS:

Q1 What is the status of Bill C-30?

A1 Bill C-30, the *Protecting Children from Internet Predators Act*, was introduced on February 14, 2012. The Bill generated significant attention from the media and privacy advocacy groups, who have been broadly critical of the proposed legislation, especially regarding the provisions compelling access to basic subscriber information. The Government announced shortly after the Bill's introduction that it would go directly to Committee after first reading. This has not yet taken place.

CONTACTS: Prepared by Marie-Helene Chayer	613-949-3181	Approved by	Tel. no.

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

s.15(1) - Int'l
s.15(1) - Subv

BRIEF ON CYBER ISSUES

[redacted]

Cyber security: Canada is concerned about the rising threats emanating from cyberspace and recognizes that partnerships with our allies and engagement at multilateral fora are critical in this respect.

Cybercrime: Canada fully supports the Council of Europe's *Convention on Cybercrime* (the *Budapest Convention*) as the best tool to fight cybercrime at the international level.

[redacted]

BACKGROUND

Cyber norms: A number of states, most prominently Russia and China, are seeking to reassert the role of the state in cyberspace, largely by arguing that concepts of national sovereignty be extended to this domain. [redacted]

Using this approach, they have sought to garner international support for this vision of cyberspace. For example, Russia has actively been pushing for the global adoption of an international information security treaty for the last decade.[1] Given cyberspace's destabilizing potential, Russia argues that a new international treaty is required to create an arms control regime to limit the proliferation of cyber weapons (however these are defined), and to prohibit cyber attacks and cyber terrorism under international law. [redacted]

[redacted]

s.15(1) - Int'l

s.15(1) - Subv

Similarly, Russia and China, supported by Tajikistan and Uzbekistan, introduced a non-binding "International Code of Conduct for Information Security" at the United Nations General Assembly in September 2011.

The U.K., , has launched an international discussion on non-binding cyber norms, which would set out the broad "rules of the road" for interactions in cyberspace. This approach seeks to reemphasize the importance existing cyber norms, such as the support for the multistakeholder model for Internet governance, and garner support for the idea that existing principles of international law (e.g. human rights law, the law of armed conflict) apply equally in cyberspace. Underpinning this normative approach to cyberspace is the idea that no major structural modifications to the cyberspace governance model or the international system are required to address new cyber issues. The London Conference on Cyberspace (November 1-2, 2011) brought together representatives from over 60 countries, the private sector and civil society to discuss a vision of cyberspace based on these high-level principles. Hungary will host the next iteration of the conference in Budapest in October 2012 and South Korea will host in 2013.

Cyber Security: The Government of Canada released Canada's Cyber Security Strategy in October 2010. Over the first five-year timeframe, the Strategy will secure Government of Canada systems, enhance partnerships to secure vital cyber systems outside the federal Government, and help protect Canadians as they connect to each other and to the world.

As part of its efforts to implement the Strategy, the Government of Canada has:

- Updated its laws to reflect the realities of the digital world by passing the *Anti-Spam Act* and creating new *Criminal Code* provisions related to identity theft.
- Introduced Bill C-30, the *Protecting Children from Internet Predators Act*, which will bring Canada in line with its international partners on lawful interception capabilities and mutual legal assistance;
- Strengthened the Canadian Cyber Incident Response Centre (CCIRC) by making it the national computer emergency response team for provinces, territories and critical infrastructure sectors;
- Engaged provincial and territorial governments to shape a joint action plan to guide collaboration on cyber security matters; and
- Developed a cyber security awareness campaign.

Cybercrime: The only international instrument that deals with cybercrime is the Council of Europe's *Convention on Cybercrime* (the *Budapest Convention*). Canada signed the Convention in 2001. In order to permit ratification of the Convention, Canada needs to make amendments to its domestic legislation. These changes are included in Bill C-30.

s.15(1) - Int'l
s.15(1) - Subv

While the Convention is trumpeted as the gold standard to combat cybercrime among Western countries, a number of states have been reluctant join on the grounds that some of its core elements, such as the 24/7 information sharing network, are deemed to violate national sovereignty. It is also on sovereignty grounds that certain countries reject provisions in the Convention that allows Parties to access stored computer data with consent of the data's host or where it is publicly available.

Some countries also view it as politically unacceptable to accede to a largely European-centric treaty, having been negotiated between members and observers of the Council of Europe. These countries believe that a global cybercrime instrument, negotiated through a United Nations process, would be more representative of a global consensus. Currently, a U.N. study group, of which a Justice Canada official is the Rapporteur, is examining the issue of cybercrime and the viability of a global treaty. The U.N. report is not expected until 2013, at the earliest.

KEY MESSAGES

Approach to cyber issues

- Canada is committed to working cooperatively with our international partners to ensure that the Internet is kept open, safe, and accessible.

- An open, safe and accessible cyberspace is key to sustaining an innovative global digital economy, and a vibrant and connected global society.

- We recognise that some activity in cyberspace can potentially threaten international peace and security. However, in addressing these issues, it is critical that we avoid taking steps that would threaten the vibrancy and openness of cyberspace.

Norms for cyberspace

- Canada is strongly supportive of the United Kingdom's efforts to foster a multistakeholder dialogue on norms for cyberspace. Canada looks forward to advancing this dialogue in Hungary in 2012 and the Republic of Korea in 2013.

s.15(1) - Int'l

s.15(1) - Subv

- Cyber norms would promote safe, predictable and consistent interactions while ensuring the Internet's unique accessibility and openness.

[redacted]

Cyber security

- Canada is concerned by the real and immediate threat posed by malicious cyber activity initiated by both state and non-state actors.

- In dealing with online threats, it is critical that states maintain strong legal checks and balances, judicial oversight and public accountability in order to safeguard human rights.

s.15(1) - Int'l

s.15(1) - Subv

- We have shared interests in making cyberspace more secure. This is a global issue and will require strong international cooperation, not only among countries, but with the private sector as well.

Cybercrime

- Canada believes the general provisions of the Council of Europe *Convention on Cybercrime* are a useful model for domestic legislation and for international cooperation.

- Canada is committed to cracking down on computer-related crime, and is working to implement the domestic requirements that would allow Canada to ratify the Council of Europe *Convention on Cybercrime*.