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.

Leclair, Natalie

From: Bedor, Tia Leigh
Sent: Thursday, June 28, 2012 6:52 AM
To: Leclair, Natalie
Cc: McAteer, Julie; Baulne, Lucie; Dupuis, Chantal
Subject: RE: NEW Petition 411-1519 - Lawful Access

Bonjour Natalie,

Please proceed with addressing this petition using existing language as suggested below.

Thanks,

Tia Leigh Bedor
Administrative Officer | *Agente Administrative*
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

---

From: Leclair, Natalie
Sent: Wednesday, June 27, 2012 3:33 PM
To: Dupuis, Chantal; Bedor, Tia Leigh; Baulne, Lucie
Cc: McAteer, Julie; Issues / Enjeux; Chang, Anna
Subject: NEW Petition 411-1519 - Lawful Access
Importance: High

Good afternoon,

Please find attached a new petition 411-1519 which was presented in the House by Ms. Savoie concerning Lawful Access.

Please note that this petition is similar to previous petitions on this subject. Please indicate if NS is comfortable with the existing response to past identical petitions. If so we will use the existing language to address this petition (previous petition 411-0970 attached).

Also attached is the prayer for this new petition.

NOTE: Please ensure that the information provided in the response to the petition is accurate and consistent with information or documents already disclosed under the *Access to Information Act* or the *Privacy Act*, or in response to other types of information requests.

Your ADM/ADM equivalent approved bilingual response should sent electronically to me with a CC to Julie McAteer **by COB on July 4, 2012**.

Please do not hesitate to contact me should you have any questions.

Thank you.
Nat

Natalie Leclair
Advisor / Conseillère
Parliamentary Affairs / Affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 990-2718
Fax: (613) 954-8774
Email/Courriel: natalie.leclair@ps-sp.gc.ca

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
411-0970	Mr. Dusseault (Sherbrooke)	May 3, 2012

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

The Honourable Vic Toews

J 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 has introduced the *Protecting Children from Internet Predators Act*.

We want to fix our laws while striking the right balance when it comes to protecting privacy.

Bill C-30 creates no new powers to access the content of e-mails or phone calls beyond that which already exists in Canadian law.

We will send this legislation directly to Committee for a full examination of potential amendments to achieve the best protection for our children.

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.

.../2

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
411-0970	M. Dusseault (Sherbrooke)	3 mai 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 la *Loi sur la protection des enfants contre les cyberprédateurs*.

Nous voulons modifier nos lois tout en établissant un juste équilibre avec la protection de la vie privée.

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.

Nous enverrons ce projet de loi directement au comité pour un examen complet d'amendements potentiels afin d'atteindre la meilleure protection pour nos enfants.

.../2

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) à 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 demandes 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.

.../3

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.

Government of Canada
Privy Council Office

Gouvernement du Canada
Bureau du Conseil privé

PETITION - PÉTITION

To / À **PUBLIC SAFETY**

Date **June 27, 2012**

SUBJECT: Petition No. / Pétition N° **411-1519**

SUJET: Member / Député **MS. SAVOIE (VICTORIA)**

Date of Petition / Date de la pétition **June 21, 2012**

FOR PRIORITY ATTENTION

Section 36 (8) of the Standing Orders:

(a) Every petition presented pursuant to this Standing Order shall forthwith be transmitted to the Ministry, which shall, within forty-five days, respond to every petition referred to it; provided that the said response may be tabled pursuant to S.O. 32(1).

(b) If such a petition remains without a response at the expiration of the said period of forty-five days, the matter of the failure of the Ministry to respond shall be deemed referred to the appropriate Standing Committee. Within five sitting days of such a referral the Chair of the committee shall convene a meeting of the committee to consider the matter of the failure of the Ministry to respond.

Would you please respond to this petition before

July 30, 2012

The response should be prepared on a "Response to Petition" form in both official languages.

If you have no information on this subject or you consider that another department should be contacted, please advise us without delay.

POUR EXAMEN PRIORITAIRE

Paragraphe 36 (8) du Règlement:

a) Toute pétition présentée conformément au présent article est transmise sur-le-champ au gouvernement, qui répond dans les quarante-cinq jours à toutes les pétitions qui lui sont renvoyées. La réponse peut être déposée conformément à l'article 32(1) du Règlement.

b) Dans le cas où une pétition reste sans réponse à l'expiration de ce délai de quarante-cinq jours, cette absence de réponse de la part du gouvernement est réputée renvoyée au comité permanent concerné. Dans les cinq jours de séance suivants ce renvoi, le président du comité convoque une réunion pour se pencher sur l'absence de réponse de la part du gouvernement.

Veuillez répondre à cette pétition avant le

La réponse doit être présentée dans les deux langues officielles sur le formulaire "Réponse à la pétition".

Si vous ne possédez aucun renseignement sur ce sujet ou si vous jugez qu'un autre ministère devrait être contacté, veuillez nous aviser sans délai.

Nicole Baker

Nicole Baker
Coordinator of Parliamentary Returns
Coordonnatrice des documents parlementaires

Canada

ASSIGNMENT: **PUBLIC SAFETY**
ASSIGNATION:

SUBJECT/SUJET

— by Ms. Savoie (Victoria), one concerning **Old Age Security benefits** (No. 411-1518), one concerning **telecommunications** (No. 411-1519) and one concerning **transportation** (No. 411-1520);	— par M^me^ Savoie (Victoria), une au sujet des **prestations de sécurité de la vieillesse** (n° 411-1518), une au sujet au sujet des **télécommunications** (n° 411-1519) et une au sujet du **transport** (n° 411-1520);

REPEAT OF 411-0970
RÉPÉTITION DE LA 411-0970

NOTE:

The subject to be typed on the form Response to Petition should be the same as the one in the Journals. (See Subject/Sujet above)

Le sujet à dactylographier sur le formulaire Réponse à la Pétition doit être le même que celui des Journaux. (Voir Subject/Sujet ci-haut)

Canada

411-1519

PETITION TO THE GOVERNMENT OF CANADA

AGAINST BILL C-30; WARRANTLESS ONLINE SPYING

We, the undersigned residents of Canada, draw the attention of the House to the following:

THAT this government, with Bill C-30, intends to engage in warrantless online spying. Such access to the private information of Internet users is a violation of our rights and freedoms as guaranteed by section 8 of the *Canadian Charter of Rights and Freedoms*, and unfairly treats all law-abiding Internet users as criminals.

THEREFORE, the petitioners urge the House of Commons not to pass Bill C-30 and to reject any proposal that would allow the authorities to obtain the private information of Internet users without a warrant.

UNCLASSIFIED

DATE: JUIL 0 4 2012

File No. : 1323-411 / 388828

MEMORANDUM FOR THE MINISTER

RESPONSE TO PETITION 411-1519
CONCERNING BILL C-30

(Signature required)

ISSUE

On June 21, 2012, Ms. Denise Savoie, M.P. (Victoria) presented a petition in the House of Commons concerning Bill C-30, *Protecting Children from Internet Predators Act* **(TAB A)**.

The response to this petition is identical to that of several other petitions on the same topic, the most recent of which was tabled in the House of Commons on May 28, 2012.

The Privy Council Office has requested a response by July 30, 2012.

The response was prepared by the Department.

RECOMMENDATION

It is recommended that you sign the attached response provided in both official languages by July 30, 2012 **(TAB B)**.

Graham Flack
Acting Deputy Minister

Enclosures: (2)

Prepared by: Natalie Leclair

Canada

Deadline for DM's signature / Échéancier pour la signature du S-M : \

Title / Titre :	**Petition 411-1519 Ms. Savoie (Victoria) Lawful Access June 21, 2012**		**ACTION REQUIRED / MESURES À PRENDRE**	
Name / Nom	**Date**	**Initials / Initiales**	**Approval or signature / Approbation ou signature**	**Information**
Originator / Auteur Natalie Leclair / Julie McAteer	June 27/12	June 25	☒	☐
Director / Directeur Jean Cintrat	JUN 28 2012	R	☒	☐
Director General / Directeur général Randall Koops	27.06.12	RK	☒	☐
Chief Audit Executive / Dirigeante principale de la vérification Rosemary Stephenson			☐	☐
Director General Communications / Directrice générale des communications Stéphanie Durand			☐	☐
Executive Director & Senior General Counsel LS / Directeur exécutif et Avocat général principal SJ Paul Shuttle			☐	☐
Assistant Deputy Minister SP / Sous-ministre adjointe PS Paul MacKinnon	June 28, 12	PM	☒	☐
Assistant Deputy Minister LP / Sous-ministre adjoint SPL Richard Wex			☐	☐
Assistant Deputy Minister CM / Sous-ministre adjointe GM Gary Robertson			☐	☐
Assistant Deputy Minister CSP / Sous-ministre adjoint SPP Shawn Tupper			☐	☐
Assistant Deputy Minister EMRO / Sous-ministre adjoint délégué SGMUOR Gina Wilson			☐	☐
Senior Assistant Deputy Minister NS/ Sous-ministre adjointe principale SN Lynda Clairmont			☐	☐
Acting Deputy Minister / Sous-ministre par intérim Graham Flack			☒	☐
Minister / Ministre The Honourable / L'honorable Vic Toews			☒	☐

411-1519

PETITION TO THE GOVERNMENT OF CANADA

AGAINST BILL C-30; WARRANTLESS ONLINE SPYING

We, the undersigned residents of Canada, draw the attention of the House to the following:

THAT this government, with Bill C-30, intends to engage in warrantless online spying. Such access to the private information of Internet users is a violation of our rights and freedoms as guaranteed by section 8 of the *Canadian Charter of Rights and Freedoms*, and unfairly treats all law-abiding Internet users as criminals.

THEREFORE, the petitioners urge the House of Commons not to pass Bill C-30 and to reject any proposal that would allow the authorities to obtain the private information of Internet users without a warrant.

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
411-1519	Ms. Savoie (Victoria)	June 21, 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

V Toews

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 has introduced the *Protecting Children from Internet Predators Act.*

We want to fix our laws while striking the right balance when it comes to protecting privacy.

Bill C-30 creates no new powers to access the content of e-mails or phone calls beyond that which already exists in Canadian law.

We will send this legislation directly to Committee for a full examination of potential amendments to achieve the best protection for our children.

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.

.../2

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
411-1519	Mme. Savoie (Victoria)	21 juin 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 la *Loi sur la protection des enfants contre les cyberprédateurs*.

Nous voulons modifier nos lois tout en établissant un juste équilibre avec la protection de la vie privée.

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.

Nous enverrons ce projet de loi directement au comité pour un examen complet d'amendements potentiels afin d'atteindre la meilleure protection pour nos enfants.

...f2

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) à 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 demandes 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.

.../3

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.

Leclair, Natalie

From: Leclair, Natalie
Sent: Thursday, September 27, 2012 10:11 AM
To: Dupuis, Chantal; Bedor, Tia Leigh; Baulne, Lucie
Cc: McAteer, Julie; Issues / Enjeux; Chang, Anna
Subject: NEW Petition 411-1784 - Lawful Access
Attachments: 411-1519 - Signed response.pdf; 411-1784-notice.doc; 411-1784 petition response.doc

Importance: High

Good afternoon,

Please find attached a new petition 411-1784 which was presented in the House by Ms. May concerning Telecommunications.

Please note that this petition is similar to previous petitions on this subject. (previous petition 411-1519 attached).

NOTE: Please ensure that the information provided in the response to the petition is accurate and consistent with information or documents already disclosed under the *Access to Information Act* or the *Privacy Act*, or in response to other types of information requests.

Your ADM/ADM equivalent approved bilingual response should sent electronically to me with a CC to Julie McAteer **by COB on October 9, 2012**.

Please do not hesitate to contact me should you have any questions.

Thank you.
Nat

Natalie Leclair
Advisor / Conseillère
Parliamentary Affairs / Affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 990-2718
Fax: (613) 954-8774
Email/Courriel: natalie.leclair@ps-sp.gc.ca

Government of Canada
Privy Council Office

Gouvernement du Canada
Bureau du Conseil privé

PETITION - PÉTITION

To / À **PUBLIC SAFETY**

Date **September 27, 2012**

SUBJECT: Petition No. / Pétition N° **411-1784**

SUJET: Member / Député **MS. MAY (SAANICH-GULF ISLANDS)**

Date of Petition / Date de la pétition **September 24, 2012**

FOR PRIORITY ATTENTION

Section 36 (8) of the Standing Orders:

(a) Every petition presented pursuant to this Standing Order shall forthwith be transmitted to the Ministry, which shall, within forty-five days, respond to every petition referred to it; provided that the said response may be tabled pursuant to S.O. 32(1).

(b) If such a petition remains without a response at the expiration of the said period of forty-five days, the matter of the failure of the Ministry to respond shall be deemed referred to the appropriate Standing Committee. Within five sitting days of such a referral the Chair of the committee shall convene a meeting of the committee to consider the matter of the failure of the Ministry to respond.

Would you please respond to this petition before

November 2, 2012

POUR EXAMEN PRIORITAIRE

Paragraphe 36 (8) du Règlement:

a) Toute pétition présentée conformément au présent article est transmise sur-le-champ au gouvernement, qui répond dans les quarante-cinq jours à toutes les pétitions qui lui sont renvoyées. La réponse peut être déposée conformément à l'article 32(1) du Règlement.

b) Dans le cas où une pétition reste sans réponse à l'expiration de ce délai de quarante-cinq jours, cette absence de réponse de la part du gouvernement est réputée renvoyée au comité permanent concerné. Dans les cinq jours de séance suivants ce renvoi, le président du comité convoque une réunion pour se pencher sur l'absence de réponse de la part du gouvernement.

Veuillez répondre à cette pétition avant le

The response should be prepared on a "Response to Petition" form in both official languages.

If you have no information on this subject or you consider that another department should be contacted, please advise us without delay.

La réponse doit être présentée dans les deux langues officielles sur le formulaire "Réponse à la pétition".

Si vous ne possédez aucun renseignement sur ce sujet ou si vous jugez qu'un autre ministère devrait être contacté, veuillez nous aviser sans délai.

Nicole Baker

Nicole Baker
Coordinator of Parliamentary Returns
Coordonnatrice des documents parlementaires

Canada

ASSIGNMENT: **PUBLIC SAFETY**
ASSIGNATION:

SUBJECT/SUJET

— by Ms. May (Saanich—Gulf Islands), one concerning **environmental assessment and review** (No. 411-1783) and one concerning **telecommunications** (No. 411-1784).	— par M^me^ May (Saanich—Gulf Islands), une au sujet de **l'examen et des évaluations environnementales** (n° 411-1783) et une au sujet au sujet des **télécommunications** (n° 411-1784).

REPEAT OF / RÉPÉTITION DE LA : 411-1519

NOTE:

The subject to be typed on the form Response to Petition should be the same as the one in the Journals. (See Subject/Sujet above)

Le sujet à dactylographier sur le formulaire Réponse à la Pétition doit être le même que celui des Journaux. (Voir Subject/Sujet ci-haut)

Canada

411-1784

PETITION TO THE HOUSE OF COMMONS

We, the undersigned residents of Canada, draw the attention of the House of Commons to the following:

THAT Canadians do not wish to allow warrantless surveillance by a range of government authorities, including access to financial and personal information, through internet and mobile devices.

THAT Federal and Provincial/Territorial Commissioners to Privacy have voiced concern that Bill C-30 will allow unacceptable intrusions into privacy rights.

THAT requiring internet and service providers to provide the information to authorities will lead to costs that will be passed on to the purchaser of the internet and mobile services, rather than borne by the authorities requesting the information.

THAT Canadians do not need a level of surveillance that is typically associated with totalitarian regimes.

THAT Canadians need privacy protection that reflects the present state of communication technology and the rights and freedoms they enjoy under the Constitution.

THEREFORE, your petitioners call upon the Government of Canada to reject those aspects of the proposed lawful access that expand surveillance, allow authorities unrestricted and warrantless access to personal information and violate the privacy of Canadians. Bill C-30 must be amended sufficiently that it is supported by federal and provincial/territorial privacy commissioners.

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
411-1519	Ms. Savoie (Victoria)	June 21, 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 has introduced the *Protecting Children from Internet Predators Act*.

We want to fix our laws while striking the right balance when it comes to protecting privacy.

Bill C-30 creates no new powers to access the content of e-mails or phone calls beyond that which already exists in Canadian law.

We will send this legislation directly to Committee for a full examination of potential amendments to achieve the best protection for our children.

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.

.../2

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
411-1519	Mme. Savoie (Victoria)	21 juin 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

Toews

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

SUBJECT / OBJET
Télécommunications

RESPONSE / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL ☐ TRANSLATION / TRADUCTION ☒

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 la *Loi sur la protection des enfants contre les cyberprédateurs*.

Nous voulons modifier nos lois tout en établissant un juste équilibre avec la protection de la vie privée.

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.

Nous enverrons ce projet de loi directement au comité pour un examen complet d'amendements potentiels afin d'atteindre la meilleure protection pour nos enfants.

.../2

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) à 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 demandes 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.

.../3

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.

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

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

Leclair, Natalie

From: Mueller, Mike
Sent: Tuesday, October 23, 2012 5:39 PM
To: McAteer, Julie
Cc: Leclair, Natalie
Subject: Re: Petition - lawful access

[redacted]

From: McAteer, Julie
Sent: Tuesday, October 23, 2012 05:37 PM
To: Mueller, Mike
Cc: Leclair, Natalie; McAteer, Julie
Subject: Re: Petition - lawful access

[redacted]

Julie McAteer
Senior Advisor, Parliamentary Affairs / Conseillère principale, affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel: 949-9737

From: Mueller, Mike
Sent: Tuesday, October 23, 2012 05:33 PM
To: Leclair, Natalie
Cc: McAteer, Julie
Subject: RE: Petition - lawful access

Public Safety Canada

[redacted]

From: Leclair, Natalie
Sent: October-23-12 12:12 PM
To: Mueller, Mike
Cc: McAteer, Julie
Subject: Petition - lawful access

As requested.

Natalie Leclair
Advisor / Conseillère
Parliamentary Affairs / Affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 990-2718
Fax: (613) 954-8774

Email/Courriel: natalie.leclair@ps-sp.gc.ca

Public Safety Canada | Sécurité publique Canada
Deputy Minister | Sous-ministre
Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: OCT 2 6 2012

File No. : 1323-411 / 390458

MEMORANDUM FOR THE MINISTER

RESPONSE TO PETITION 411-1784
CONCERNING BILL C-30

(Signature required)

ISSUE

On September 24, 2012, Ms. Elizabeth May, M.P. (Saanich—Gulf Islands) presented a petition in the House of Commons concerning Bill C-30, *Protecting Children from Internet Predators Act* **(TAB A)**.

The response has been updated to reflect the status of the current legislation.

The Privy Council Office has requested a response by November 2, 2012.

The response was prepared by the Department.

RECOMMENDATION

It is recommended that you sign the attached response provided in both official languages by November 2, 2012 **(TAB B)**.

Graham Flack
Acting Deputy Minister

Enclosures: (2)

Prepared by: Natalie Leclair

Canada

Public Safety Canada / Sécurité publique Canada

SPB / CPES

DEPUTY MINISTER'S OFFICE
PUBLIC SAFETY CANADA
2012 OCT 04 A 9:55

Routing Slip / Bordereau d'acheminement

File No / No de dossier : DEP- 390458

Deadline for DM's signature / Échéancier pour la signature du S-M : _____

Title / Titre : Petition 411-1784 Ms. May (Saanich-Gulf-Islands) Telecommunications September 27, 2012

ACTION REQUIRED / MESURES À PRENDRE

Name / Nom	Date	Initials / Initiales	Approval or signature / Approbation ou signature	Information
Originator / Auteur Natalie Leclair/Julie McAteer	oct.10		☒	☐
Director / Directeur Jean Cintrat	22-10-12	EC.	☒	☐
Director General / Directeur général *Randall Koops*	22-X-12	RAK	☒	☐
Chief Audit Executive / Dirigeante principale de la vérification Rosemary Stephenson			☐	☐
Director General Communications / Directrice générale des communications *Stéphanie Durand*			☐	☐
Executive Director & Senior General Counsel LS / Directeur exécutif et Avocat général principal SJ Paul Shuttle			☐	☐
Assistant Deputy Minister SP / Sous-ministre adjointe PS Paul MacKinnon	24 oct. 12	PM	☒	☐
Assistant Deputy Minister LP / Sous-ministre adjoint SPL Richard Wex			☐	☐
Assistant Deputy Minister CM / Sous-ministre adjointe GM Gary Robertson			☐	☐
Assistant Deputy Minister CSP / Sous-ministre adjoint SPP Shawn Tupper			☐	☐
Assistant Deputy Minister EMRO / Sous-ministre adjoint délégué SGMUOR *Gina Wilson*			☐	☐
Senior Assistant Deputy Minister NS/ Sous-ministre adjointe principale SN Lynda Clairmont			☐	☐
Acting Deputy Minister / Sous-ministre par intérim Graham Flack			☒	☐
Minister / Ministre The Honourable / L'honorable Vic Toews			☒	☐

411-1784

PETITION TO THE HOUSE OF COMMONS

We, the undersigned residents of Canada, draw the attention of the House of Commons to the following:

THAT Canadians do not wish to allow warrantless surveillance by a range of government authorities, including access to financial and personal information, through internet and mobile devices.

THAT Federal and Provincial/Territorial Commissioners to Privacy have voiced concern that Bill C-30 will allow unacceptable intrusions into privacy rights.

THAT requiring internet and service providers to provide the information to authorities will lead to costs that will be passed on to the purchaser of the internet and mobile services, rather than borne by the authorities requesting the information.

THAT Canadians do not need a level of surveillance that is typically associated with totalitarian regimes.

THAT Canadians need privacy protection that reflects the present state of communication technology and the rights and freedoms they enjoy under the Constitution.

THEREFORE, your petitioners call upon the Government of Canada to reject those aspects of the proposed lawful access that expand surveillance, allow authorities unrestricted and warrantless access to personal information and violate the privacy of Canadians. Bill C-30 must be amended sufficiently that it is supported by federal and provincial/territorial privacy commissioners.

Canada

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. 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.

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. 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.

Champoux, Elizabeth

From: Champoux, Elizabeth
Sent: Monday, November 05, 2012 8:32 AM
To: Champoux, Elizabeth
Subject: Lawful Access Article - CACP Jim Chu Op-Ed

http://www.infomedia.gc.ca/ps-sp/articles/unrestricted/2012/11/ps-201211811476160_16.htm

Beth Champoux
Senior Advisor, Parliamentary Affairs / Conseillère principale, affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 949-1058
Email/Courriel: elizabeth.champoux@ps-sp.gc.ca

Provided by NewsDesk http://www.infomedia.gc.ca/ps-sp/ Fourni par InfoMédia

Published | Publié: 2012-11-05
Received | Reçu: 2012-11-05 4:18 AM

CALGARY HERALD

CALGARY HERALD (FINAL)
THE EDITORIAL PAGE, Page: A13

New law is about safety, not about snooping

Jim Chu, Calgary Herald

As **Canadians**, we rightly place a very high value on our privacy.

As a career **police** officer, I have spent much of my life ensuring that my actions and those of the officers under my command do not intrude into the privacy of others, unless authorized by law and in pursuit of those who threaten, harm or steal from others.

While all new laws should be subject to rigorous debate, I worry that the misinformation surrounding the proposed Bill **C-30**, Protecting Children from Internet Predators Act, is distracting us from the true goal of this bill - protecting **victims** by updating laws last introduced by Parliament in 1974. At that time, telecommunications consisted of rotary phones, telegraphs and physical lines of wire. A technology revolution has seen the rapid adoption of mobile devices, computers and social media - an evolution of technology not envisaged by lawmakers back in the 1970s.

Canadians reap many benefits from today's technologies. So do criminals. We have inadvertently created safe havens for those who exploit technology to traffic in weapons, drugs and people. It is a boon to pedophile networks, money launderers, extortionists, deceitful telemarketers, **fraudsters** and **terrorists**. Cyber bullies communicate their vitriol with impunity. If we stand by and do nothing, criminals will continue to use these interactive platforms to harass and threaten others, commit **frauds**, scams and organized and violent crimes with little fear of being caught.

I enthusiastically agree that privacy is a right to cherish and guard vigorously. We believe that the new legislation, with our recommended amendments to strengthen privacy rights, will help make **Canada** a safer place. To level the playing field for **law enforcement**, successive federal governments introduced updated **lawful access** legislation in 2006, 2007, 2009 and 2010. All of these bills died on the order paper. In the meantime, the threats to individuals and community are increasing. The current proposed legislation includes the following assurances/improvements:

- Access to private information will continue to require a judicial authorization (warrant);

- Telecommunications providers will be required to preserve data while a warrant is being obtained;

- Basic subscriber information (the equivalent to information provided by a telephone directory) will be obtainable in a timely and consistent manner. As opposed to today's environment, the new legislation builds in an audit trail to ensure **accountability** (including making available reporting to the judiciary and privacy commissioners) and to limit those within **policing** who can make such a request.

What is the cost of not proceeding with the modernization of our laws? Organized criminals will plan their killings and kidnappings using communications providers whose systems do not have the technical ability to be monitored through the warrant process. **Terrorists** will be able to exploit these same gaps. **Victims** of scams will be told that the evidence trail linking the suspect to the **crime** has disappeared because the service provider has no obligation to preserve data.

Perhaps even worse, the parents of a child who has been lured or criminally harassed over the Internet will learn that the **police** investigation will be delayed or be completely unsuccessful because of the need to obtain a warrant for basic subscriber information. The **RCMP's** National **Child Exploitation** Co-ordination Centre looked at a sample of 1,244 requests for basic subscriber information in 2010. The average response time to gain such information was 12 days. This is unacceptable.

The challenge of Bill **C-30** is to strike the right balance between providing **law enforcement** with investigative tools to ensure individual and **public safety** while ensuring the protection of privacy. We support the greater protections that have been built into this bill. It is illegal for **police** to randomly snoop on **Canadians**. This does not change with the new legislation.

Can the bill be improved? Absolutely, and we support a provision to clarify privacy rights. Do **police** in **Canada** support unwarranted Internet surveillance or snooping? Absolutely not!

Parliament has the opportunity to bring **law enforcement** powers into the 21st century. **Canadian police** chiefs have spoken up in the name of the **victims** of **crime** we encounter every day. If the laws are not modernized, I assure **Canadians** we will still do our jobs to the best of our ability, but there will be less **policing** capacity, fewer cases prosecuted, more **victims of crime**, and more unsolved cases. Criminals will like that.

Will you?

Jim Chu is chief constable of the Vancouver **Police** Department and president of the **Canadian Association of Chiefs of Police**. ILLUS: / Jim Chu;

Thompson, Julie

From: Plunkett, Shawn
Sent: Wednesday, February 27, 2013 10:55 AM
To: Chayer, Marie-Helene
Cc: Thompson, Julie
Subject: FW: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

Spoke with Zarah and tomorrow is fine for us to provide them with something.

They did note that the normal service standard is 72 hours, however, they were very delayed (nearly two weeks) in providing us the request (original request was Feb 14).

Therefore, there will likely be some pressure if we can't get something to them tomorrow.

From: Thompson, Julie
Sent: February-26-13 3:39 PM
To: Plunkett, Shawn
Cc: Chayer, Marie-Helene
Subject: RE: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

Hi,
Zarah mentioned that the response can wait for tomorrow. In the meantime, let me know if I can prepare anything.

Julie

Julie Thompson
Policy Analyst/Analyste en politiques
Investigative Technologies and Telecommunications Policy/Politiques sur les technologies d'enquête et les télécommunications
National Security Operations Directorate/Direction des Operations de Sécurité Nationale
Public Safety Canada/Sécurité Publique Canada
Tel: 613.998.7893
Email/Courriel : julie.thompson@ps-sp.gc.ca

From: Plunkett, Shawn
Sent: February-26-13 3:11 PM
To: Thompson, Julie
Cc: Chayer, Marie-Helene
Subject: Fw: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

Please see below.
Can you find out from comms if they need it today or can it wait for tomorrow?

If needed urgently, I provided a package to comms a couple of months ago that included the SGES. I think I sent it to you as well.

Thank you.
Shawn Plunkett

[redacted]
PS/SP Canada

s.19(1)

From: Hawrylak, Maciek
Sent: Tuesday, February 26, 2013 02:55 PM
To: Communications_; Day, Liliane
Cc: Picard, Josée; Plunkett, Shawn
Subject: Re: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

Hello Zarah,

Liliane may have already responded, but my colleague Shawn Plunkett handles the SolGen standards.

Best,
Maciek

From: Communications_
Sent: Tuesday, February 26, 2013 01:27 PM
To: Day, Liliane
Cc: Communications_; Hawrylak, Maciek; Picard, Josée
Subject: FW: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

Hello Ms. Day,
As Maciek is away, would you be able to help with the enquiry below?
We would be grateful for any direction you could provide.
Thank you for your time.

Zarah Malik
613-949-5536

From: Communications_
Sent: Tuesday, February 26, 2013 1:26 PM
To: Hawrylak, Maciek
Cc: Communications_; Picard, Josée
Subject: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

Hello Maciek,

I was referred to you by my colleague at NS, Chris Willey.
I'm hoping that you might be able to help respond to the public enquiry below.
Would you know where we might be able to retrieve a copy of the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications?
We would appreciate any direction you could provide, thank you.

Name	[redacted]
Enquiry Date	2/14/2013
Language	English
Phone #	
Location	Ontario

E-mail	[redacted]@gmail.com s.19(1)
Type of Enquiry	Related to Public Safety
Method of Enquiry	E-mail
Organization	
PS Branch	
Program	
Portfolio Agency/Review Bodies	
Questions	Hello, I would like to obtain a copy of the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications, along with any proposed changes. It says at http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10473.html " For further information on proposed changes to the Solicitor General's Enforcement Standards, please contact Public Safety Canada via the General Enquiries line at 1-800-830-3118." I decided to try to contact you by electronic means first but will telephone if necessary.

Zarah Malik

Agente des communications | Communications Officer
Gestion des enjeux, Affaires publiques | Issues Management Team, Public Affairs Division
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-5536 | F : 613-954-4779

Emmett, Jamie

From: Chayer, Marie-Helene
Sent: February-27-13 4:44 PM
To: Durand, Mathieu
Subject: RE: Rapports sur les interceptions en France.

Tracking:	**Recipient**	**Read**
	Durand, Mathieu	Read: 27/02/2013 4:48 PM

Merci beaucoup Mathieu.

Je vais rentrer à la maison plus tôt à cause de la température. Mais j'ai bien hâte d'entendre ton histoire de pantalon demain...

Bonne soirée

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

From: Durand, Mathieu
Sent: February-27-13 4:37 PM
To: Chayer, Marie-Helene
Subject: Rapports sur les interceptions en France.

Marie-Hélène,

Grosso modo, il y a deux types d'interceptions en France. Les interceptions de sécurité (elles visent à prévenir un acte) et les interceptions judiciaires. Certains rapports de la Commission nationale de contrôle des interceptions de sécurité sont disponibles en ligne. [redacted]

Ainsi, de l'information à propos des [redacted] serait la bienvenue.

s.21(1)(a)

Mathieu Durand
Policy Analyst / Analyste des politiques
Investigative Technologies and Telecommunications Policy / Technologies d'enquêtes et politiques des télécommunications
National Security Operations Directorate / Direction générale des opérations de la sécurité nationale
Public Safety Canada / Sécurité publique Canada
613-990-8020 / Mathieu.Durand@ps-sp.gc.ca

Thompson, Julie

From: Thompson, Julie
Sent: Tuesday, February 26, 2013 3:27 PM
To: Chayer, Marie-Helene
Cc: Plunkett, Shawn
Subject: RE: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Hi
I have contacted comms and left a voice mail message. Will keep you posted.

Julie

Julie Thompson
Policy Analyst/Analyste en politiques
Investigative Technologies and Telecommunications Policy/Politiques sur les technologies d'enquête et les télécommunications
National Security Operations Directorate/Direction des Operations de Sécurité Nationale
Public Safety Canada/Sécurité Publique Canada
Tel: 613.998.7893
Email/Courriel : julie.thompson@ps-sp.gc.ca

From: Chayer, Marie-Helene
Sent: February-26-13 3:16 PM
To: Thompson, Julie
Subject: FW: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Julie,

Voici ce dont Shawn parle dans son courriel. On ne donne pas de copie du documents. Peux-tu contacter comms?

Merci

MH

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

From: Plunkett, Shawn
Sent: January-02-13 3:40 PM
To: Duval, Jean Paul
Cc: Champoux, Martin; MacDonald, Michael; Kingsley, Michèle; Chayer, Marie-Helene
Subject: FW: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Hi JP,
Please find enclosed the following document related to the below request:

1) The annotated copy of the Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications.

2) A backgrounder contextualizing the SGES. This document is for background use for PS comms only and should not be shared.

3) A comms package written for our proposed modifications to the "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications" (SGES). This package was developed with and previously submitted to comms.

4) A Primer on Spectrum in Canada (background material on what is spectrum)

Please note that these documents are for internal use only and should not be shared with the applicant.

This package was approved by our acting DG.

Please let me know should you require anything further.

Shawn

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques
Investigative Technologies and Telecommunications Policy (ITTP) /
Technologies d'enquêtes et politiques des télécommunications (TEPT)
National Security Operations Directorate / Direction des opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
Tel: (613) 990-7066
Email: shawn.plunkett@ps.gc.ca

From: MacDonald, Michael
Sent: January-02-13 9:11 AM
To: Maillé, Marie Anick
Cc: Kingsley, Michèle; Chayer, Marie-Helene; Plunkett, Shawn
Subject: Fw: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Hi,

Can you pls action this. In providing the document to Comms for them to read, you might think about also attaching the Primer as well.

Merci. MM

From: Duval, Jean Paul
Sent: Monday, December 31, 2012 03:47 PM
To: MacDonald, Michael
Cc: Champoux, Martin
Subject: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Good day Mike,

We received a request from the Globe and Mail seeking an interview/discussion on specific interception standards for telecommunication carriers as detailed in the "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications".

Comms would like to start by reviewing this document. Can you advise if someone within your team can provide a copy for our reference? FYI - MO is also interested in reviewing this document.

Kind regards,
JP

Title	[redacted]
Media Outlet	Globe and Mail
Call Date	12/31/2012 3:00 PM
Telephone	[redacted]
E-mail address	[redacted]@globeandmail.com
Deadline	Oper
Status	Consulting
Subject	Lawful Interception Enforcement Standards (re: Lawful Access)
Questions	I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008. I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible? **Document info**: - "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table." - said to be "current as of Nov. 17 2008" - 22 standards make explicit what the government is seeking from telecom networks and carriers - Annotated with italics further explaining the standards - Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc) - Prepared by Public Safety's National Security Technology Division

s.19(1)

Jean Paul Duval
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-1689
Cell | Portable: [redacted]
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

Thompson, Julie

From: Chayer, Marie-Helene
Sent: Tuesday, February 26, 2013 3:16 PM
To: Thompson, Julie
Subject: FW: Media Call - Globe and Mail - Lawful Interception Enforcement Standards
Attachments: PS-SP-#526559-12-COMMS - Standard Comms Responses - 700MHz Auction, SGES Modifications.DOC; PS-SP-#586039-10-A Primer on Spectrum in Canada - Virtual Library - 2012-03-20.DOC; PS-SP-#748449-5-Backgrounder - SGES - 2012-01-02.DOCX; PS-SP-#469348-1-Standard - SolGen Enforcement Standards for Lawful Interception of Telecommunications - ANNOTATED.PDF

Julie,

Voici ce dont Shawn parle dans son courriel. On ne donne pas de copie du documents. Peux-tu contacter comms?

Merci

MH

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

From: Plunkett, Shawn
Sent: January-02-13 3:40 PM
To: Duval, Jean Paul
Cc: Champoux, Martin; MacDonald, Michael; Kingsley, Michèle; Chayer, Marie-Helene
Subject: FW: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Hi JP,
Please find enclosed the following document related to the below request:

1) The annotated copy of the Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications.

2) A backgrounder contextualizing the SGES. This document is for background use for PS comms only and should not be shared.

3) A comms package written for our proposed modifications to the "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications" (SGES). This package was developed with and previously submitted to comms.

4) A Primer on Spectrum in Canada (background material on what is spectrum)

Please note that these documents are for internal use only and should not be shared with the applicant.

This package was approved by our acting DG.

Please let me know should you require anything further.

Shawn

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques
Investigative Technologies and Telecommunications Policy (ITTP) /
Technologies d'enquêtes et politiques des télécommunications (TEPT)
National Security Operations Directorate / Direction des opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
Tel: (613) 990-7066
Email: shawn.plunkett@ps.gc.ca

From: MacDonald, Michael
Sent: January-02-13 9:11 AM
To: Maillé, Marie Anick
Cc: Kingsley, Michèle; Chayer, Marie-Helene; Plunkett, Shawn
Subject: Fw: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Hi,

Can you pls action this. In providing the document to Comms for them to read, you might think about also attaching the Primer as well.

Merci. MM

From: Duval, Jean Paul
Sent: Monday, December 31, 2012 03:47 PM
To: MacDonald, Michael
Cc: Champoux, Martin
Subject: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Good day Mike,

We received a request from the Globe and Mail seeking an interview/discussion on specific interception standards for telecommunication carriers as detailed in the "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications".

Comms would like to start by reviewing this document. Can you advise if someone within your team can provide a copy for our reference? FYI - MO is also interested in reviewing this document.

Kind regards,
JP

s.19(1)

Title	[redacted]
Media Outlet	Globe and Mail
Call Date	12/31/2012 3:00 PM
Telephone	[redacted]
E-mail address	[redacted]@globeandmail.com
Deadline	Open
Status	Consulting

Subject

Lawful Interception Enforcement Standards (re: Lawful Access)

Questions

I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008.

I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible?

Document info:
- "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table."
- said to be "current as of Nov. 17 2008"
- 22 standards make explicit what the government is seeking from telecom networks and carriers
- Annotated with italics further explaining the standards
- Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc)
- Prepared by Public Safety's National Security Technology Division

Jean Paul Duval
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-1689
Cell | Portable: [redacted]
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

s.19(1)

(Current as of 17/11/2008)

s.15(1) - Subv
s.16(1)(b)
s.16(2)

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

Solicitor Generals Standards

Standard 1: Law enforcement agencies require access to the entire telecommunications transmitted, or caused to be transmitted, to and from the number or other identifier of the target service used by the interception subject. Law enforcement agencies also require access to the call-associated data that is generated to process the call.

Standard 2: Law enforcement agencies require access to all mobile interception subjects operating temporarily or permanently within a telecommunications system.

Standard 3: Law enforcement agencies require access in cases where the interception subject may be using features to divert calls to other telecommunications service or terminal equipment, including calls that traverse more than one network or are processed by more than one network operator/service provider before completing.

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

[redacted]

Standard 4: Law enforcement agencies require that the telecommunications to and from a target service be provided to the exclusion of any telecommunications that do not fall within the scope of the interception authorization.

[redacted]

Standard 5: Law enforcement agencies require access to available call associated data such as:

A) Signaling of access ready status

[redacted]

B) Called party number for outgoing connections even if there is no successful connection established

[redacted]

s.15(1) - Subv
s.16(1)(b)
s.16(2)

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

C) Calling party number for incoming connections even if there is no successful connection established

[redacted]

D) All digits dialed by the target, including post-connection dialed digits used to activate features such as conference calling and call transfer

[redacted]

E) Beginning, end, and duration of the connection

[redacted]

F) Actual destination and intermediate directory numbers if call has been diverted.

(Current as of 17/11/2008)

s.15(1) - Subv
s.16(1)(b)
s.16(2)

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

[redacted]

Standard 6: Law enforcement agencies require information on the most accurate geographical location known to the network for mobile subscribers.

[redacted]

Standard 7: Law enforcement agencies require data on the specific service used by the interception subject and the technical parameters for that type of communication.

[redacted]

Standard 8: Law enforcement agencies require a real- time, full-time monitoring capability for the interception of telecommunications. Call associated data should also be provided in real-time. If call associated data cannot be made available in real time, law enforcement agencies require the data to be

available as soon as possible upon call termination.

[redacted]

Standard 9: Law enforcement agencies require network operators/service providers to provide one or more interfaces from which the intercepted communications can be transmitted to the law enforcement monitoring facility. These interfaces have to be commonly agreed on by the interception authorities and the network operators/service providers. Other issues associated with these interfaces will be handled according to generally accepted practices.

[redacted]

Standard 10: Law enforcement agencies require network operators/service providers to provide call associated data and call content from the target service in a way that allows for the accurate correlation of call associated data with call content.

[redacted]

(Current as of 17/11/2008)

s.15(1) - Subv
s.16(1)(b)
s.16(2)

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

[redacted]

Standard 11: Law enforcement agencies require that the format for transmitting the intercepted communications to the monitoring facility be a generally available format.

[redacted]

Standard 12: If network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications en clair.

[redacted]

Standard 13: Law enforcement agencies require network operators/service providers to be able to transmit the intercepted communications to the law enforcement monitoring facility via fixed or switched connections.

[redacted]

s.15(1) - Subv
s.16(1)(b)
s.16(2)

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

[redacted]

Standard 14: Law enforcement agencies require that the transmission of the intercepted communications to the monitoring facility meet applicable Government of Canada security requirements.

[redacted]

Standard 15: Law enforcement agencies require interceptions to be implemented so that neither the interception target nor any other unauthorized person is aware of any changes made to fulfill the interception order. In particular, the operation of the target service must appear unchanged to the interception subject.

[redacted]

Standard 16: Law enforcement agencies require the interception to be designed and implemented to preclude unauthorized or improper use and to safeguard the information related to the interception.

[redacted]

Standard 17: Law enforcement agencies require network operators/service providers to protect information on which and how many interceptions are being or have been performed, and not disclose information on how interceptions are carried out.

(Current as of 17/11/2008)

s.15(1) - Subv
s.16(1)(b)
s.16(2)

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

[redacted]

Standard 18: Law enforcement agencies require network operators/service providers to ensure that intercepted communications are only transmitted to the monitoring agency specified in the interception authorization.

[redacted]

Standard 19: Based on a lawful inquiry and before implementation of the interception, law enforcement agencies require **(1)** the interception subject's identity service number or other distinctive identifier, **(2)** information on the services and features of the telecommunications system used by the interception subject and delivered by network operators/service providers, and **(3)** information on the technical parameters of the transmission to the law enforcement monitoring facility.

[redacted]

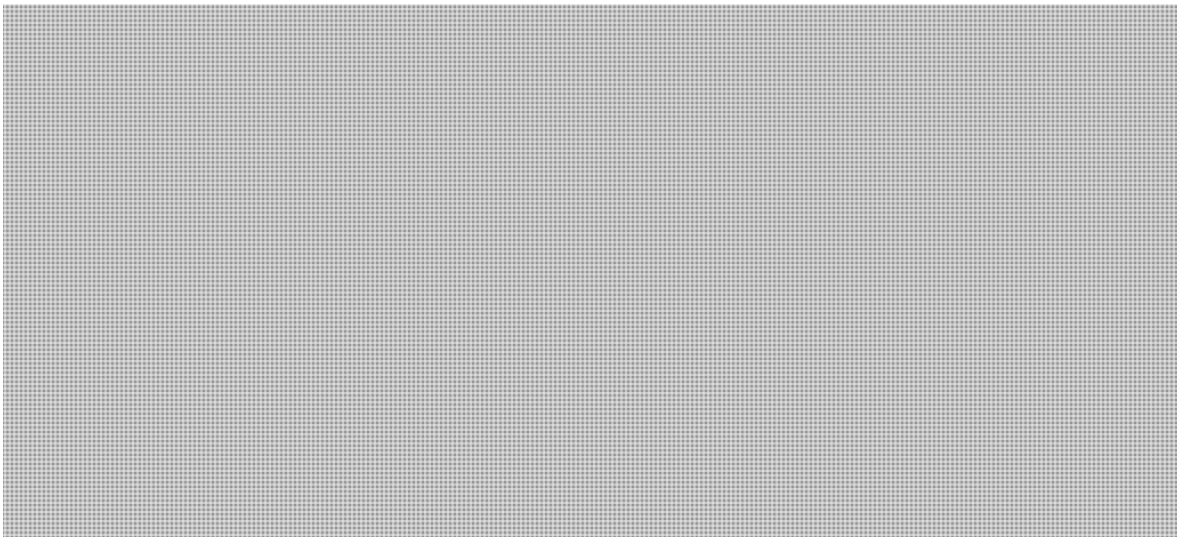
Standard 20: During the interception law enforcement agencies may require information and/or assistance from the network operators/service providers to ensure that the communications acquired at the interception interface are those communications associated with the target service.

[redacted]

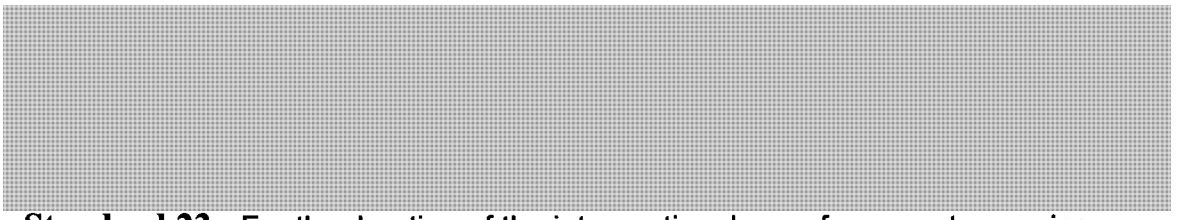
Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

s.15(1) - Subv
s.16(1)(b)
s.16(2)

Standard 21: Law enforcement agencies require network operators/service providers to make provisions for implementing a number of simultaneous intercepts. Multiple interceptions may be required for a single target service to allow monitoring by more than one law enforcement agency. In this case, network operators/service providers should take precautions to safeguard the identities of the monitoring agencies and ensure the confidentiality of the investigations.



Standard 22: Law enforcement agencies require network operators/service providers to implement interceptions as quickly as possible (in urgent cases within a few hours or minutes). The response requirements of law enforcement agencies will vary by the type of target service to be intercepted.



Standard 23: For the duration of the interception, law enforcement agencies require that the reliability of the services supporting the interception at least equals the reliability of the target services provided to the interception subject. Law enforcement agencies require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the network operators/service providers.

(Current as of 17/11/2008)

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

s.15(1) - Subv
s.16(1)(b)
s.16(2)

Public Consultation to the 700 MHz and 2500 MHz Spectrum Auction

Public Enquiries/Media Relations Messages

ISSUE:

Industry Canada (IC) is planning an auction anticipated for the first half of 2013 to allocate spectrum in the 700 MHz and a further auction on the 2500 MHz bands likely the following year. Prior to this auction, a second public consultation in 2012 on the design of the 700 MHz and the 2500 MHz auctions will be held. Specifically, IC will be consulting on what conditions will be attached to the spectrum licences for the 700 and 2500 MHz band. In this context, we have been working to include a lawful interception condition of licence and to remove from this condition any reference to "circuit-switched voice telephony". Also, Public Safety Canada (PS) indicated to IC that it will be proposing minor modifications to the guidelines document that outlines intercept capability requirements entitled: *Solicitor General Enforcement Standards for Lawful Interception of Telecommunications (Sol Gen Standards),* as they were last revised in 1995.

s.21(1)(a)

With respect to the *Sol Gen Standards*, PS had indicated to IC that we would be proposing [redacted] minor modifications to the standards. [redacted] but will indicate in its public consultation that PS proposes to modernize these standards and refer stakeholders to PS for further information. We have proposed to IC that they include the PS General Enquiries phone line in the public consultation document to handle any public enquiries regarding these proposed changes.

As a result, we expect that affected companies may contact Public Safety Canada to enquire as to proposed changes to the *Sol Gen Standards.* It should be noted that Public Safety cannot respond to questions surrounding the auction writ large or on any specific condition of licence. Public Safety Canada is only responsible for the *Sol Gen Standards.* Please note that while not a classified document, due to the nature of the material, there is sensitivity regarding actively publicizing the *Sol Gen Standards.*

PROTOCOL

For Media Relations:

- When a call is received by Media Relations, a notification will be sent to the Minister's Office Director of Communications, the DG of Communications, program communications strategists and the responsible policy sector.
- Media Relations spokespeople will use the messages and Q&As below to formulate responses and work with the policy sector to finalize answers.
- Final media lines need to be approved by the DG NS Ops or as delegated.

- Media Relations will then seek approvals from DG Communications and the Minister's Office as well as advise PCO Communications.
- Once approved, media relations will provide the final response to the journalist.

For Public Enquiries:

- Calls are logged as they are received and responded to using the initial method of contact (phone or email). For straightforward questions, Public Enquiries officers will provide the preapproved responses provided below.
- For calls seeking to provide feedback or more complex questions, Public Enquiries can forward requests to the policy centre.
- Public Enquiries will provide the policy sector with updates on number of calls received on request.

MEDIA LINES:

Public Safety Canada is proposing minor modifications to the *Solicitor General Enforcement Standards for Lawful Interception of Telecommunications*.

s.21(1)(a)

While the changes are minor, we are currently seeking feedback from targeted stakeholders to ensure that their views are heard.

STANDARD RESPONSES FOR PUBLIC ENQUIRIES

If caller is requesting any information relating to the 700 MHz or 2500 MHz Spectrum auction:

- Industry Canada is responsible for the public consultation on the spectrum auctions. Should you wish to make comments on the spectrum auction, please contact Industry Canada.

If caller is requesting any information relating to the Lawful Interception Condition of Spectrum Licence:

- Industry Canada is responsible for the public consultation on the conditions of licences. Should you wish to make comments on the condition of licence, please contact Industry Canada.

If caller is seeking a copy of the SolGen Standards:

- Please provide us with your contact information and the responsible party at Public Safety will contact you shortly.

[*Please forward along contact information and any relevant notes to the policy centre for further action.*]

If caller is seeking what changes are being made to the SolGen Standards:

- Public Safety Canada has informed Industry Canada that it is proposing modifications to the *Solicitor General Enforcement Standards for Lawful Interception of Telecommunications.*

- Public Safety Canada is seeking feedback on potential modifications from targeted stakeholders in order to seek their views on any potential changes. At this time, we are proposing only minor modifications to the *Solicitor General Enforcement Standards* that we expect will have little impact on licensees.

    - **If further details are requested**:

      We would be happy to take your contact information and the responsible party at Public Safety will contact you in the near future.

If caller is seeking to make comments on proposed changes to the SolGen Standards

- We welcome your input into the proposed changes. We would be happy to take your contact information and have the responsible party at Public Safety contact you in the near future.

Qs & As:

When will these proposed changes take effect?
Notifications will be sent to licencees should any changes to the *Solicitor General Enforcement Standards* be made.

How will these changes affect the spectrum auction?
These changes will not have any direct bearing on the spectrum auction themselves.

Will removing "Circuit-Switched" have a significant impact on our business?
The removal of the term 'circuit-switched' forms part of the conditions of licence and not the *Solicitor General Enforcement Standards*. Industry Canada is responsible for the public consultation on the conditions of licence. Should you wish to make comments on the conditions of licence, please contact Industry Canada.

UNCLASSIFIED

DATE:

File No.: NS 6652
RDIMS No: 586039

MEMORANDUM FOR THE DIRECTOR GENERAL

A PRIMER ON SPECTRUM IN CANADA

(Information only)

ISSUE

This memo will provide background information on spectrum and its properties, specifically with respect to the 700 MHz and 2500 MHz bands. It will also provide information as to how spectrum is managed in Canada.

BACKGROUND

This primer was developed through open sources materials by Public Safety officials.

What is Spectrum?
Spectrum or radio spectrum is radio frequencies on which all communication signals travel, including wireless services, GPS, radio, television, etc. Spectrum is, in basic terms, the highway over which voice, data, images and other communications travel. It is a finite resource and in today's digital age is the backbone of our economy and our lifestyles. The increased use by consumers, as well as the increase in the number of services requiring spectrum, means that spectrum demand is increasingly outpacing supply. Dropped calls, lag times and slow upload or download speeds can all be attributable to limited spectrum.

Spectrum is made up of various frequencies, the unit for which is the hertz (Hz). The frequency is determined by the number of complete waves past a fixed point in one second. Thus, the frequency of a signal where 700 million waves pass a fixed point in one second is 700 MHz.

Spectrum Ranges
Spectrum frequencies are grouped into ranges, each of which possesses particular characteristics that determine its usage. While there are 12 different ranges as designated by the International Telecommunications Union (ITU, the UN body responsible for international spectrum management- see below for more on spectrum management), popular telecommunications services operate in the Ultra High Frequency (UHF) range. The range of the UHF is 300 MHz to 3000 MHz. Both the 700 and 2500 MHz spectrum frequencies fall within the UHF band.

Frequency Bands
The UHF range is separated into smaller frequency bands. In Canada, the following bands in the UHF range are designated for commercial mobile services:

- Mobile Broadband Services (MBS): 698-764 / 776-794 MHz (700 MHz Band)
- Cellular: 824-849 / 869-894 MHz ('Cel' or 800 MHz Band)
- Advanced Wireless Services (AWS): 1710-1755 / 2110-2155 MHz
- Personal Communications Services (PCS): 1850-1915 / 1930-1995 MHz
- Broadband Radio Services (BRS): 2500-2690 MHz (2500 MHz Band)

These bands are very similar to the bands designated in the U.S., with slight modifications for the Canadian market. Industry Canada allocates spectrum largely along U.S. lines to help ensure interoperability, harmonization and equipment complementarity. Bands are sometimes given a 'common name', such as Cellular or PCS, to differentiate between the frequency bands. However, the name does not necessarily limit the type of equipment that can operate over the bands (i.e. cellular phones can operate on other bands besides the 'Cel' band). Some of the uses of the other frequency bands not listed above in the UHF include: television and radio, air traffic control radars, mobile satellite services, paging, search and rescue satellites, among others. Each band has certain characteristics, which make it more useful to one service or another.

Capacity
The lower frequencies have the longest radio waves and the higher frequencies have the shortest radio waves. Lower frequencies are longer highways, but cannot carry as much information. Higher frequencies are shorter highways, but can carry more information- i.e. they have more broadband capacity. This means that services that carry a lot of information (such as wireless internet connections for the home and mobile data services) are better placed in the higher frequency bands while signals with less information (such as voice, text or radio) can be carried by the lower frequency bands.

Propagation
Another factor that differentiates spectrum bands is its propagation characteristics. Propagation refers to the way radio waves behave as they travel from point to point

While there are several other factors relating to propagation, one of the key factors relates to how much power is transmitted. Since waves continue until they run out of power, the more power each wave has, the further it can go. Lower frequencies are said to travel longer distances because they have more power. A combination of both the length (lower frequencies have longer waves) and the power of the waves are what likely contribute to the ability of these frequency bands to penetrate through walls and buildings.

Bandwidth
Bandwidth is the range of frequencies that a signal occupies in the spectrum- i.e. the width of the cars on the highway. For example, an FM radio station might broadcast on a frequency of 92.9 MHz but requires a bandwidth of 0.3 MHz (the frequencies 92.8, 92.9 and 93.0 MHz). Other stations cannot broadcast on these frequencies within the same region without causing or receiving interference. Voice or texting takes less bandwidth than data services, such as downloading a movie or video, which means that more calls/text can be sent at the same time within a proscribed spectrum range.

SPECTRUM MANAGEMENT

Industry Canada (IC) is responsible for the management of the radio frequency spectrum and satellite orbital resources. Access to these resources is provided through authorization. The growth in the number and variety of applications, along with ever-increasing user expectations, places an increasing demand on the radio frequency spectrum and thus the need to manage it effectively and efficiently.

Given that radio frequency emissions are not bound by geopolitical boundaries, spectrum must also be effectively coordinated on a global scale. In this context, Canada participates in various international governmental organizations such as the International Telecommunication Union (ITU), where the treaty-binding *ITU Radio Regulations* (RR) are developed and updated. The RR provides a basis for the *Canadian Table of Frequency Allocations* (CTFA), which establishes the frequency allocations available for radio services in Canada. While the CFTA reflects international changes, it also takes into account Canadian requirements to ensure that government, commercial and private users have full flexibility to develop new applications.

Spectrum Blocks
As part of spectrum management, IC further classifies frequency bands into blocks of spectrum. Through the development of a 'band plan', and in conjunction with international standards and regulations, IC assigns different blocks of spectrum for different purposes. These purposes include: being auctioned off for commercial use; held for public safety purposes; held for public goods, such as air traffic control radars or meteorological uses; assigned as guard bands to limit interference between blocks; or

reserved as unusable blocks (simply meaning that there are no known uses or technology for this part of the spectrum). In developing a band plan, IC must take several factors into consideration when assigning spectrum including the size of the blocks, the 'pairing' of blocks and the equipment and technology that is available on frequency bands.

Spectrum Block Size

Returning to the highway analogy, how wide the highways are (narrow or broadband) and whether they are built for one way or two way traffic (paired or unpaired) are critical for the efficient use of spectrum, in terms of access, speed and volume of traffic. Sending large amounts of information (music, video) requires broadband (large blocks), while smaller amounts of information (voice, texts) can make use of narrower bands of spectrum. Yet, as spectrum is a fixed resource, the band plan must also consider the distribution and allocation of spectrum. For example, creating fewer, larger blocks of spectrum (broadbands), may allow for more information to pass through, but would limit the number of companies or organizations with access to the spectrum (i.e. it would be limited to the company that successfully bid on the spectrum). As there are rules governing spectrum sharing and interference between blocks, it is difficult, and often not in the best interests of the successful bidder, to share spectrum. Conversely, if there are many, smaller blocks of spectrum, it would increase access to the spectrum by different parties, but would limit the usefulness of spectrum by constricting the amount of information that could pass through each block. For the 700 MHz band, IC publicly consulted on which 'band plan', should be adopted. It was decided that the band plan that proposed harmonization with the U.S. band plan will be adopted for the 700 MHz. This harmonization will also ensure that there is considerable equipment and technology available that is compatible with the frequencies as well as ensuring cross-border roaming.

Paired and unpaired (uplink and downlink)

Also taken into consideration when allocating spectrum is whether the spectrum traffic is paired (where all the traffic in the block goes one-way, either upload or download) or unpaired (where the traffic can go both ways). Paired spectrum allocates two distinct and equal frequency blocks; one assigned to "downlink", (from the base station to mobile devices), and the other to "uplink" (from the mobile device to the base station). Voice traffic works well in paired spectrum, as it has roughly the same amount of information travelling in the uplink as it does for the downlink (i.e. you 'upload' your voice to your counterpart in one block of spectrum and 'download' their voice from another block). In contrast, unpaired spectrum provides a single block used for both downlink and uplink (most people download information off the Internet, but fewer upload information). Data services, such as web pages, content, video, music, etc., tend to have considerable more information travelling on the downlink side, meaning that unpaired spectrum is more efficient for this type of use.

Regions/ Tiers

Finally, in Canada, mobile service providers are granted spectrum licences to allow them to provide coverage over a specific geographic area. In Canada, these geographic areas

(often called tiers or service areas) define the boundaries of the spectrum licence. Therefore, one national wireless carrier will need to hold many spectrum licences, one for each different service area. Breaking spectrum licences into smaller service areas allows for regional and smaller providers to bid on licences that coincide with their business plans. For example, SaskTel and MTS Allstream can bid on spectrum licences in the service areas for Saskatchewan and Manitoba or WIND Mobile and Mobilicity can bid for spectrum only in Toronto and Montreal if they so choose. However, the more service areas there are, the increased likelihood there will be for interference between neighbouring service areas (simply because there will be more shared 'borders' between areas). For the 700 MHZ auction, IC publicly consulted on the size and location of the tiers. In the recent decision paper, it was decided that there will be 14 services areas (roughly based on provinces, with one area for all the territories and several additional areas for the high density urban populations in southern Ontario, Ottawa-Gatineau and Montreal).

700 and 2500 MHz SPECTRUM

All spectrum bands have positive and negative characteristics. How one describes 'prime' spectrum is essentially a matter of trade-offs; sacrificing distance for volume of information for example. The 700 MHz spectrum comprises 108 MHz of spectrum, the frequencies from 698-806 MHz. It was previously used for analog television, but is being re-purposed for commercial and public safety use. The appeal of the 700 MHz band is that it is a 'middle ground' band. It is a low enough frequency to travel far and penetrate through buildings, yet high enough to be able to transmit a sufficient level of data.

Some of the pros of the 700 MHz band as assigned by IC are:

- Can travel longer distances than the previous spectrum for wireless. This reduces the number of signal transmitting towers needed, thus reducing costs of building and maintaining infrastructure, especially when delivery to rural communities.

- Can penetrate buildings and walls, due to the properties of the frequency. This is especially useful in downtown, urban areas.

- In the 700 MHz band, IC has carved out 4 blocks of paired spectrum, referred to as 'Prime' spectrum (blocks: B, C, C1, C2):

    - These blocks are paired and therefore are good for delivering voice/cell phone services;

- The size of these bands range from 10 and 12 MHz, which is sufficient (although not optimal) to run LTE networks; 20 MHz is the highest range for LTE and therefore would make for the fastest network.

- Blocks B and C correspond with the blocks used by AT&T in the U.S. Therefore, equipment and devices that are manufactured to work on AT&T's large network will be compatible in Canada. This provides economies of scale, where Canadian telecommunications companies will not need standalone or custom equipment or devices for their own networks. In addition, having corresponding spectrum and equipment will facilitate roaming between countries.

- Blocks C1 and C2 correspond with the blocks used by Verizon. This is beneficial for the same reasons as above.

Some of the pros of the 2500 MHz band as assigned by IC are:

- This spectrum will be able to transmit a considerable amount of broadband data to users as higher frequencies can transmit more data.

- There is a significant amount of spectrum available- nearly 200 MHz of spectrum.

- The unpaired blocks will be large- 25 MHz each.

- While the paired blocks will be only 10 MHz, due to the number of blocks available, there is the possibility that companies can purchase neighbouring blocks, thus giving them a wider spectrum to use.

Prepared by: Shawn Plunkett
May 29, 2012

MEDIA CALL - LAWFUL INTERCEPTION ENFORCEMENT STANDARDS

BACKGROUND

Spectrum is, in basic terms, the highway over which voice, data, images and other communications travel. It is a finite resource and in today's digital age is the backbone of our economy and our lifestyles. The increased use by consumers, as well as the increase in the number of services requiring spectrum, means that spectrum demand is increasingly outpacing supply. Dropped calls, lag times and slow upload or download speeds can all be attributable to limited spectrum.

In Canada, as in many other countries, spectrum is often allocated by way of auction and managed through a licencing regime, whereby successful bidders are given spectrum licences. Under the *Radiocommunication Act*, the Minister of Industry has the authority to grant spectrum licences and place conditions on these licences. Licence holders must comply with these conditions in order to use their purchased spectrum to provide wireless services, such as cellular and internet services. A component of this licensing framework is the lawful interception condition of spectrum licence, which requires licence holders to have and maintain lawful interception capabilities. This lawful interception condition is the primary instrument for public safety agencies to compel applicable telecommunications companies to effect court authorized intercepts.

Part of the lawful interception condition of licence is for licence holders to comply with the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications* (SGES) - a set of 23 requirements that serves as a technical guide for telecommunications companies on how to provide public safety agencies with lawful intercepts. They range from what type of information law enforcement and national security agencies require the licence holder to provide, the technical information as to how it must be provided, and security parameters that must be followed. Due to differences in network architecture, law enforcement and national security agencies must often work with the individual licence holders to discuss these standards. It should also be noted that due to the nature of the material in the document, there is sensitivity regarding publishing the SGES. They are not a public document and are not available on any Government of Canada website.

s.16(1)(c)
s.16(2)

The lawful intercept condition of licence has limitations, however. [redacted]

CURRENT STATUS

To address limitations outlined above, Public Safety Canada (PS) and Industry Canada (IC) are examining ways to revise the lawful interception condition and have publicly consulted on proposed changes as part of the upcoming 700 and 2500 MHz auctions. While we are working with IC to update the lawful interception condition for new technologies that can be used for

future spectrum auctions, any potential changes will not apply to existing licences, but only to future licences on the 700 and 2500 MHz bands.

As part of a larger consultation on all the licence conditions that are being proposed to apply to the 700 and 2500 MHz spectrum bands, IC has publicly consulted on the lawful interception condition of licence. These public consultations allowed stakeholders to comment on the expected conditions that will be assigned to the 700 MHz and 2500 MHz spectrum licenses. Included in the language of these consultations was that PS is proposing minor modifications to the SGES. These proposed modifications, however, were not formally part of IC's public consultation, which was limited to only the conditions of spectrum licence.

Public consultations on the 700 MHz auction occurred in May-July 2012 and for the 2500 MHz auction in October-December 2012. Taking into account these public consultations, IC is currently deliberating on the proposed changes to the condition of licences. A decision on whether to make any proposed changes to the lawful interception condition of licence for the 700 MHz auction is expected in early 2013, while a decision on the 2500MHz auction is expected later in 2013. These decisions will not change the SGES; they will only impact the lawful interception condition of licence.

All comments made as part of these consultations were made public on IC's website. Many of the telecommunications companies that provided comments were opposed to making changes to
s.16(1)(c) the lawful interception condition of licence,
s.16(2) Many also noted that any changes to the lawful interception regime in Canada should be done through legislation.

Hawrylak, Maciek

From: Keating, Sarah
Sent: Tuesday, February 26, 2013 9:09 AM
To: Chayer, Marie-Helene
Cc: Hawrylak, Maciek
Subject: RE: Lawful Access Bill item

Importance: High

s.21(1)(a)

Classification: SECRET//CANADIAN EYES ONLY

Bonjour Marie-Hélène et Maciek,
Ma note en vue de la rencontre du ministre avec le MI5 a bloqué au bureau du sous-ministre. [redacted]
Est-ce que je pourrais vous demander de fournir rapidement quelques lignes pour ajouter à la note et un message clé correspondant?
Merci,
Sarah

De : Chayer, Marie-Helene
Envoyé : 15 février 2013 11:37
À : Keating, Sarah; Hawrylak, Maciek
Cc : Hirsch, Darryl
Objet : RE: Lawful Access Bill item

Classification: SECRET//CANADIAN EYES ONLY

Bonjour Sarah,
J'en ai parlé à Ritu et on s'était pas mal entendu sur le contenu de la note. Je ne pense pas que le Ministre ait besoin de plus de contexte - c'est pas mal frais dans sa mémoire...

Laisse-moi savoir si tu veux en discuter davantage.

Bonne journée,

MH

From: Keating, Sarah
Sent: Friday, February 15, 2013 11:28 AM
To: Hawrylak, Maciek
Cc: Hirsch, Darryl; Chayer, Marie-Helene
Subject: RE: Lawful Access Bill item

Classification: SECRET//CANADIAN EYES ONLY

Hi Maciek,
Thank you for your contribution. This is useful, however, we need to be able to give to the minister some context on this issue here in Canada and a sens of where the bill withdrawal leaves us.
Could you please ad that side of the story to your contribution?
Many thanks,
Sarah

De : Hawrylak, Maciek
Envoyé : 15 février 2013 10:13
À : Keating, Sarah

Cc : Hirsch, Darryl; Chayer, Marie-Helene
Objet : RE: Lawful Access Bill item

Classification: SECRET//CANADIAN EYES ONLY

Sarah,

Please find attached, for use in your BN, our input with a brief background section and two Talking Points.

Best,
Maciek

Maciek Hawrylak
National Security Operations Directorate | Direction des opérations de sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel. | tél 613-991-6036
Fax. | téléc 613-990-2632
maciek.hawrylak@psepc.gc.ca

<< Fichier: Lawful Access - Minister meeting with MI5 - 2013-03-00.doc >>

From: Keating, Sarah
Sent: Wednesday, February 13, 2013 2:25 PM
To: Hawrylak, Maciek
Cc: Hirsch, Darryl
Subject: Lawful Access Bill item
Importance: High

Classification: SECRET//CANADIAN EYES ONLY

Hi Maciek,

Your colleague Shaun indicated that you are the analyst working on the Lawful Access Act.

I am preparing a briefing note for the Minister in view of his meeting with the Director General of MI5 (U.K.'s national security intelligence agency).

Based on discussions with officials at the British High Commission, the issue of the withdrawal of the Lawful Access Bill was raised as a topics of interest for discussion during this visit.

Could I ask you to provide us with an input and key messages on this item by **noon, Friday February 15**?

Thank you very much in advance.

Sarah

Sarah Keating
Policy Analyst - Analyste des politiques
Intelligence Policy Division - Direction des politiques du renseignement
National Security Policy Directorate - Direction générale des politiques du renseignement
Public Safety Canada - Sécurité publique Canada
Tel: 613-998-2899

Hawrylak, Maciek

From: Hawrylak, Maciek
Sent: February-07-13 9:14 AM
To: Schofield, Jennifer; Kwavnick, Andrea
Subject: RE: Lawful Access PIA

Hi Jennifer,

I would say that it remains on hold. We have no further clarity on when/if the bill (or some derivative thereof) will move forward, so absent any further information, I would suggest we keep it on the books.

Thanks,
Maciek

Maciek Hawrylak
National Security Operations Directorate | Direction des Operations de Sécurité Nationale
Public Safety Canada | Sécurité Publique Canada
Tel | Tél : 613-991-6036
Fax | Téléc : 613-991-4669
Maciek.Hawrylak@ps-sp.gc.ca

From: Schofield, Jennifer
Sent: February-07-13 7:58 AM
To: Hawrylak, Maciek; Kwavnick, Andrea
Subject: RE: Lawful Access PIA

Good morning!

Last year, about this time, I had inquired about the status of this PIA. I am again gearing up for year end and reporting requirements, so am wondering about the status of this. Has it been abandoned for the moment, or is it still just on hold?

Any information you can provide is appreciated.

Thanks,

Jennifer Schofield
ATIP Coordinator/Coordonnatrice d'AIPRP
Public Safety Canada/Sécurité publique Canada
Tel/tél 613-991-2929
Fax/télécopieur 613-954-5167
Email/courriel Jennifer.Schofield@ps-sp.gc.ca

From: Nixon, Jennifer
Sent: February-23-12 9:42 AM
To: Hawrylak, Maciek; Kwavnick, Andrea
Subject: RE: Lawful Access PIA

Thank you.

I'll likely be checking back in April as we have to report on PIAs in our Annual Reports to Parliament and to TBS, so want to make sure it is either continuing, or has been abandoned at that time,

Thanks again!

Jennifer Nixon
ATIP Coordinator/Coordonnatrice d'AIPRP
Public Safety Canada/Sécurité publique Canada
Tel/tél 613-991-2929
Fax/télécopieur 613-954-5167
Email/courriel Jennifer.Nixon@ps-sp.gc.ca

From: Hawrylak, Maciek
Sent: February-23-12 9:40 AM
To: Nixon, Jennifer; Kwavnick, Andrea
Subject: RE: Lawful Access PIA

Jennifer,

With the introduction of C-30, we will shortly be turning our attention back the PIA. However, with the Bill potentially undergoing amendments, I would highly doubt we'll have something before end of fiscal, and likely only sometime in the summer months.

Thanks,
Maciek

Maciek Hawrylak
National Security Operations Directorate | Direction des Operations de Sécurité Nationale
Public Safety Canada | Sécurité Publique Canada
Tel | Tél : 613-991-6036
Fax | Téléc : 613-991-4669
Maciek.Hawrylak@ps-sp.gc.ca

From: Nixon, Jennifer
Sent: February-22-12 8:29 AM
To: Hawrylak, Maciek; Kwavnick, Andrea
Subject: Lawful Access PIA

Good morning,

As we are coming closer to the end of fiscal, I'm wondering if you can please update me on the status of the lawful access PIA

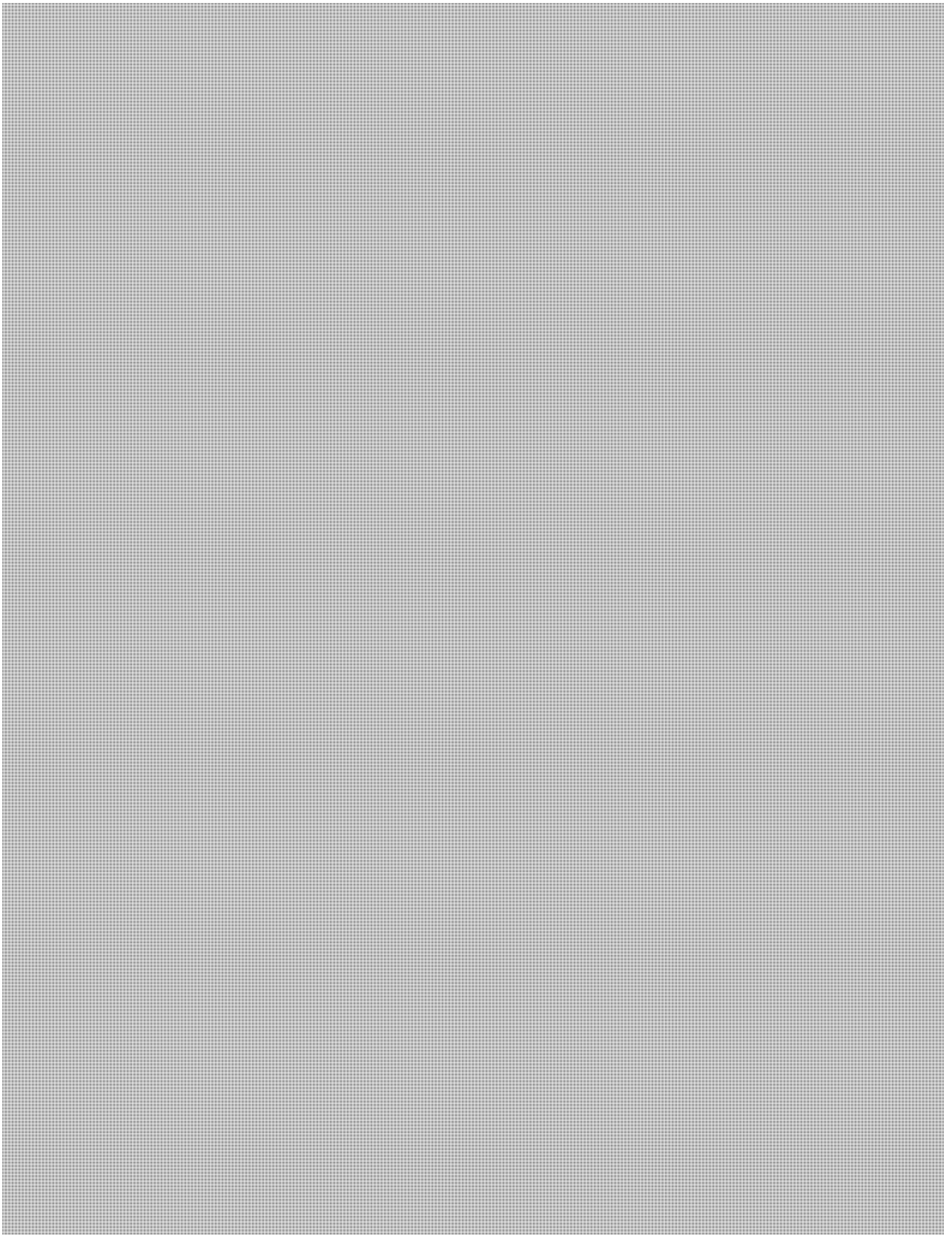
Thanks

Jennifer Nixon
ATIP Coordinator/Coordonnatrice d'AIPRP
Public Safety Canada/Sécurité publique Canada
Tel/tél 613-991-2929
Fax/télécopieur 613-954-5167
Email/courriel Jennifer.Nixon@ps-sp.gc.ca

s.21(1)(a)

SECRET
Advice to Minister
s.21(1)(a) of *ATI Act* applies
06 Feb 2013

ISSUE



Hawrylak, Maciek

From: Audcent, Karen <Karen.Audcent@justice.gc.ca>
Sent: January-09-13 4:25 PM
To: Hawrylak, Maciek
Subject: FW: (Info only) (Lawful access) E-mails show Public Safety staffers stunned when Internet surveillance bill was put on ice

---

From: Bryden, Cathleen
Sent: 2013-Jan-09 3:07 PM
To: Audcent, Karen; Nguyen, Trang Dai
Subject: (Info only) (Lawful access) E-mails show Public Safety staffers stunned when Internet surveillance bill was put on ice

Anna Mehler Paperny

The Globe and Mail

Published Wednesday, Jan. 09 2013, 10:39 AM EST

Last updated Wednesday, Jan. 09 2013, 11:25 AM EST

When the federal Conservatives announced they were sending a web surveillance bill back to the drawing board, ministry staff working on the bill found out through news reports that evening.

Bill C-30, which would make it easier for police to track Canadians online, sparked a firestorm of protest when it was unveiled in early 2012 over accusations it abrogated privacy rights. In the face of that opposition the government sent the bill back to committee for revision instead of along to second reading. This opened it up to a wide range of amendments – and a much longer time frame – before being passed.

That decision caught many Public Safety staffers unawares, documents obtained by The Globe and Mail through an access to information request suggest. Further e-mails indicate bureaucrats scrambled afterwards to tweak Conservative talking points to fit the new direction.

On Feb. 15, 2012, after days of vitriolic debate over the cybercrime bill during which he accused opponents of standing "with the child pornographers," Public Safety Minister Vic Toews took a much more conciliatory tone: "We will send this legislation directly to committee for a full and wide-ranging examination of the best way to do what is right for our children," he said in Question Period.

Just before 8 p.m. that evening, someone from the Competition Bureau e-mailed several Public Safety Ministry staffers inquiring about a Globe article saying the bill would skip second reading and go directly to committee. "Do you have any information on this and possible timing?" he asked.

"First I've heard of it," replied a policy adviser.

(Subsequent e-mails that evening found other media organizations had the same information but yielded little else.)

The temporary confusion illustrates just how quickly the Tories changed tack on a bill that went from being a major part of their majority government agenda to a piece of legislation in limbo, still awaiting amendments a year after it was brought forward in its latest form.

In the weeks following his announcement, Public Safety staffers massaged existing talking points to reflect the change in course: "There is a nuance we would like you to convey in these nine speeches" being prepared for Tory MPs to read during debates, a senior Public Safety adviser wrote in a directive to speechwriters Feb. 24. "The bill will be called at second reading but will *not* be read a second time. … Although the Minister cannot speak to pointed amendments the government is considering in the speeches, he can indicate that the government is open to considering virtually any amendment at Committee."

There was further confusion as to how much emphasis to put on the government's backtrack in revised speeches. "We have only made a passing reference of sending this Bill to Committee in one speech," a Feb. 29 e-mail from a speech unit manager reads. "Should we be making the reference at all?"

The same senior adviser replied later that afternoon:

"I might be inclined touch upon the significance of the Bill being sent directly to Committee in the speeches, given the fact the Minister has made numerous public declarations on this matter."

The change of plan also caused deadline headaches as staffers in the Public Safety and Justice ministries scrambled to prepare briefings under an uncertain time frame.

"We note that the Motion to move the Bill directly to Committee is not yet on the Order Paper, and may not be for some time (but who knows)," reads one Public Safety e-mail responding to a request for quick turnaround. "Until we have a good sense of when the Motion will be debated … we would appreciate more time to perfect the various deliverables we are managing."

The federal government is working with federal privacy watchdog Jennifer Stoddart to make the bill more palatable to its opponents, the Canadian Press reported this week. Critics of the legislation, Ms. Stoddart and her Ontario counterpart included, argue it violates Canadians' rights by giving police easy access to their information with insufficient judicial oversight.

The bill would allow police and intelligence officers access to a person's name, address, telephone number, e-mail address and Internet Protocol address without a warrant. Right now, Internet service providers give that information voluntarily.

Under the legislation, Internet service providers would need to be able to monitor user activity in real time – a potentially expensive investment that telcos hope Ottawa will help fund.

Emmett, Jamie

From: Maillé, Marie Anick
Sent: January-02-13 10:22 AM
To: Hawrylak, Maciek
Subject: Fw: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Bonjour Maciek,
Can you call me please. [redacted]
Hope things are all right.
Anick
P.s. Happy new year!!

s.19(1)

From: MacDonald, Michael
Sent: Wednesday, January 02, 2013 09:10 AM
To: Maillé, Marie Anick
Cc: Kingsley, Michèle; Chayer, Marie-Helene; Plunkett, Shawn
Subject: Fw: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Hi,

Can you pls action this. In providing the document to Comms for them to read, you might think about also attaching the Primer as well.

Merci. MM

From: Duval, Jean Paul
Sent: Monday, December 31, 2012 03:47 PM
To: MacDonald, Michael
Cc: Champoux, Martin
Subject: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Good day Mike,

We received a request from the Globe and Mail seeking an interview/discussion on specific interception standards for telecommunication carriers as detailed in the "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications".

Comms would like to start by reviewing this document. Can you advise if someone within your team can provide a copy for our reference? FYI - MO is also interested in reviewing this document.

Kind regards,
JP

Title	[redacted]
Media Outlet	Globe and Mail
Call Date	12/31/2012 3:00 PM
Telephone	[redacted]

E-mail address	[redacted]
Deadline	s.19(1)
Status	Open
Subject	Consulting
	Lawful Interception Enforcement Standards (re: Lawful Access)
Questions	I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008. I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible? **Document info**: - "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table." - said to be "current as of Nov. 17 2008" - 22 standards make explicit what the government is seeking from telecom networks and carriers - Annotated with italics further explaining the standards - Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc) - Prepared by Public Safety's National Security Technology Division

Jean Paul Duval
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-1689
Cell | Portable: [redacted]
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

Hawrylak, Maciek

From: Pierre Piche <Pierre.Piche@rcmp-grc.gc.ca>
Sent: November-01-12 8:53 AM
To: Hawrylak, Maciek
Cc: Mark Flynn; William Beiersdorfer
Subject: Fwd: RE: Lawful Access Options

s.21(1)(a)
s.21(1)(b)

Hi again Maciek,

[redacted]

Thanks,
Pierre

>>> Pierre Piche 2012-11-01 07:42 >>>
Correct. [redacted]
Pierre

>>> "Hawrylak, Maciek" <Maciek.Hawrylak@ps-sp.gc.ca> 2012-10-31 09:00 >>>
Pierre,

Thanks. Is it safe to assume the preferred option for the RCMP would still be Option 4, and that a combination of 2 and 3 is acceptable?

Maciek

From: Pierre Piche [mailto:Pierre.Piche@rcmp-grc.gc.ca]
Sent: October-31-12 8:54 AM
To: Hawrylak, Maciek
Subject: Lawful Access Options

Hi Maciek,

[redacted]

Hope this helps,
Pierre

s.16(2)

Hawrylak, Maciek

From: Chartrand, Francine <Francine.Chartrand@ppsc-sppc.gc.ca>
Sent: October-30-12 1:29 PM
To: Hawrylak, Maciek
Cc: Hattem, Tina
Subject: RE: Lawful Access - PMR

Welcome, Maciek, and thank you for the update.

Francine

Francine Chartrand
Directrice, Planification stratégique et gestion du rendement /
Director, Strategic Planning and Performance Management
Direction générale des poursuites réglementaires et économiques, et de la gestion / Regulatory and Economic Prosecutions and Management Branch
Service des poursuites pénales du Canada / Public Prosecution Service of Canada
2258-284 rue Wellington Street
Ottawa, Ontario K1A 0H8
Tél. / Tel. 613-946-7991 Télec / Fax 613-946-9977
Courriel / E-mail Francine.Chartrand@ppsc-sppc.gc.ca
Gouvernement du Canada / Government of Canada

From: Hawrylak, Maciek [mailto:Maciek.Hawrylak@ps-sp.gc.ca]
Sent: October 30, 2012 12:21 PM
To: [redacted] Nguyen, Trang Dai; Audcent, Karen; Shogilev, Matthew; [redacted] Chartrand, Francine; Hattem, Tina; 'Lisa.Foley@ic.gc.ca' (Lisa.Foley@ic.gc.ca); 'Bruce.Wallace@ic.gc.ca' (Bruce.Wallace@ic.gc.ca); Andre Leduc (Leduc.Andre@ic.gc.ca) (Leduc.Andre@ic.gc.ca); Pierre Piche (Pierre.Piche@rcmp-grc.gc.ca); Mark Flynn (mark.flynn@rcmp-grc.gc.ca); Kousha, Hasti; Cameron, Frank
Cc: Chayer, Marie-Helene
Subject: RE: Lawful Access - PMR

Dear colleagues,

As most of you know, I have assumed the lawful access file from Andrea. I'm pleased to advise you that we received unofficial confirmation this morning from TBS that their Assistant Secretary has accepted the PMR for this year. An official confirmation letter should be sent within the next few weeks, and we will ensure that you receive a copy.

Best regards,
Maciek

Maciek Hawrylak
National Security Operations Directorate | Direction des Operations de Sécurité Nationale
Public Safety Canada | Sécurité Publique Canada
Tel | Tél : 613-991-6036
Fax | Téléc : 613-991-4669
Maciek.Hawrylak@ps-sp.gc.ca

From: Kwavnick, Andrea [mailto:Andrea.Kwavnick@ps-sp.gc.ca]
Sent: August 20, 2012 10:08 AM
To: [redacted] Nguyen, Trang Dai; Audcent, Karen; Shogilev, Matthew; [redacted] Chartrand, Francine; Hattem, Tina; Bruce.Wallace@ic.gc.ca; 'Andre.Leduc@ic.gc.ca' (Andre.Leduc@ic.gc.ca); Pierre Piché (pierre.piche@rcmp-grc.gc.ca); Sgt. Mark Flynn (mark.flynn@rcmp-grc.gc.ca); Kousha, Hasti; Cameron, Frank
Cc: Haeck, Kimberly
Subject: Lawful Access - Performance Measurement Report

Good Morning,

The PMR has been approved at the PS DG level (Director General of the National Security Operations Directorate) and is ready to be approved by your respective ADMs.

As indicated in the critical path that was sent out at the beginning of this process, please send me an email indicating ADM-level approval by Tuesday, August 28th.

It is necessary that approval be granted by August 28th in order to have sufficient time for the report to be approved by TBS before the September 15th deadline.

Please note that two small changes were made in the Introduction:

1 – pg. 8 - under Legislation/Policy Documents; second last line used to read "a significant portion of the policy work..." this was changed to "a significant portion of the regulatory work..."

2 – pg. 8 – under Consultation/Outreach; the following sentence was added: "Many partners also took part in discussions with representatives of the telecommunications industry through a Government Industry Collaborative Forum that was created in 2012."

Below are the ADM-level officials who signed off on the report last year. Please let me know if there have been any changes:

Antoine Babinsky - Royal Canadian Mounted Police
[redacted] Canadian Security Intelligence Service s.16(2)
[redacted] - Communications Security Establishment Canada
Donald Piragoff - Department of Justice
George Dolhai - Public Prosecution Service Canada
Susan Bincoletto - Industry Canada

RCMP/CSIS/CSEC – the report will be sent over secure email.
IC/PPSC/DoJ – please contact Kim Haeck to pick up a disk.

Thank you very much for your help putting this year's report together. Please give me a call if you have any questions.

Andrea

Andrea Kwavnick
Senior Policy Analyst, Investigative Technologies and Telecommunications Policy |
Conseillère principale en politiques, Technologies d'enquêtes et politiques des télécommunications
National Security Operations | Opérations de la sécurité nationale
Public Safety Canada | Sécurité publique Canada
613.949.6169 / Andrea.Kwavnick@ps.gc.ca

McKinnon, Korey

From: Hawrylak, Maciek
Sent: October-26-12 10:55 AM
To: Chayer, Marie-Helene
Cc: Maillé, Marie Anick; Scott, Marcie
Subject: RE: CACP Lawful Access Docs - Todays Media Conf - 1:00 p.m. EST

The CACP media package includes 3 documents:

1. Media Release: a 2-page document that describes in general terms why lawful access is needed and why the current system doesn't work. It's a relatively cogent piece. It references the utility of lawful access to investigate all types of crimes increasing planned or committed online, including murder, kidnapping, extortion, fraud, child exploitation, and child bullying. It does suggest that Section 34 (inspection) be modified to make it clear that the intent of the passage is to ensure compliance with the law (and perhaps to remove the ability to intercept communications).
2. Lawful Access backgrounder: a 15-page document which goes over the basics of the legislation, includes a chart comparing today's rules and procedures for accessing information and any changes (or not) as proposed in the bill, important facts about the legislation (primarily what it won't do), a long Q&A designed to dispel myths and focusing on BSI, several cases demonstrating the utility of BSI and interception, and a reprint of the Federal Ombudsman for the Victims of Crime's statements in 2011 calling for mandatory provision of BSI. While there are a few errors in the document, it is largely accurate and helps simplify the issues for the general public. We have, for the most part, similar products and lines, except that ours were never released.
3. Media Advisory: provides details regarding today's press conference.

Maciek

From: Chayer, Marie-Helene
Sent: October-26-12 9:44 AM
To: Hawrylak, Maciek
Cc: Maillé, Marie Anick; Scott, Marcie
Subject: FW: CACP Lawful Access Docs - Todays Media Conf - 1:00 p.m. EST
Importance: High

More stuff. Please take a look and let me know what you think.

Thanks

Marie

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: MacDonald, Michael
Sent: October-26-12 9:42 AM
To: Chayer, Marie-Helene
Subject: FW: CACP Lawful Access Docs - Todays Media Conf - 1:00 p.m. EST
Importance: High

From: Timothy Smith [mailto:timsmith2000@rogers.com]
Sent: October-26-12 9:22 AM

To: Genevieve Breton; Julie.Vaux@pmo-cpm.gc.ca; Mueller, Mike; Jarmyn, Tom
Subject: CACP Lawful Access Docs - Todays Media Conf - 1:00 p.m. EST
Importance: High

Final Documentation fyi.

Please find attached the related English and French documentation being distributed at the CACP Media Conference being held today on Lawful Access at 1:00 EST. Note that it is be web-cast the www.vpd.ca website at that time. Info is being posted at www.CACP.ca

- Video: Police Confirm Canadians' Top 5 Fears about Lawful Access / La police confirme les cinq plus grandes craintes des Canadiens au sujet du projet de loi C-30

English
http://youtu.be/ymVqkugH8PU

French:
http://youtu.be/w5U1_LsUBeU

- Media Advisory: "We Can't Stand By And Do Nothing!"
- Media Release: Police Confirm Canadians' Top Five Fears About Lawful Access - CACP Renews Appeal for Lawful Access Legislation

Emmett, Jamie

From: Chayer, Marie-Helene
Sent: October-26-12 9:44 AM
To: Hawrylak, Maciek
Cc: Maillé, Marie Anick; Scott, Marcie
Subject: FW: CACP Lawful Access Docs - Todays Media Conf - 1:00 p.m. EST
Attachments: E1 Final CACP Press Release - Lawful Access.pdf; ATT00001.htm; E Final - CACP Media Advisory Vancouver - Lawful Access.pdf; ATT00002.htm; E Simplifying Lawful Access final english.pdf; ATT00003.htm; f_Final - CACP Media Advisory Vancouver - Lawful Access.pdf; ATT00004.htm; f1_Final CACP Press Release - Lawful Access.pdf; ATT00005.htm; F Simplifier l'acces legal finale francais.pdf; ATT00006.htm

Importance: High

More stuff. Please take a look and let me know what you think.

Thanks

Marie

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: MacDonald, Michael
Sent: October-26-12 9:42 AM
To: Chayer, Marie-Helene
Subject: FW: CACP Lawful Access Docs - Todays Media Conf - 1:00 p.m. EST
Importance: High

From: Timothy Smith [mailto:timsmith2000@rogers.com]
Sent: October-26-12 9:22 AM
To: Genevieve Breton; Julie.Vaux@pmo-cpm.gc.ca; Mueller, Mike; Jarmyn, Tom
Subject: CACP Lawful Access Docs - Todays Media Conf - 1:00 p.m. EST
Importance: High

Final Documentation fyi.

Please find attached the related English and French documentation being distributed at the CACP Media Conference being held today on Lawful Access at 1:00 EST. Note that it is be web-cast the www.vpd.ca website at that time. Info is being posted at www.CACP.ca

- Video: Police Confirm Canadians' Top 5 Fears about Lawful Access / La police confirme les cinq plus grandes craintes des Canadiens au sujet du projet de loi C-30

English
http://youtu.be/ymVqkugH8PU

French:
http://youtu.be/w5U1_LsUBeU

- Media Advisory: "We Can't Stand By And Do Nothing!"
- Media Release: Police Confirm Canadians' Top Five Fears About Lawful Access - CACP Renews Appeal for Lawful Access Legislation

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

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

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. Law Enforcement is seeking consistency and ensuring that the TSP's are not the ones who randomly decide what we can, or cannot, investigate.*

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.

Examples of the need for interception capability

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

AVIS AUX MÉDIAS

POUR DIFFUSION IMMÉDIATE

L'Association canadienne des chefs de police réitère son appel à l'action : « Nous ne pouvons pas rester à rien faire! »

Vancouver (Colombie-Britannique) – Le vendredi 26 octobre 2012, le chef Jim Chu, président de l'Association canadienne des chefs de police (ACCP) tiendra une conférence de presse nationale au sujet de l'accès légal, qui fait l'objet du projet de loi C-30, la « *Loi sur la protection des enfants contre les cyberprédateurs* ».

Le chef Chu et d'autres participants seront disponibles pour des entrevues à l'issue de la conférence de presse.

Date / heure : Vendredi 26 octobre 2012, 10 h à 11 h (heure du Pacifique)

Lieu : Salle des médias, 1er étage, Service de police de Vancouver, 2120, rue Cambie, Vancouver (Colombie-Britannique)

Veuillez noter que cette conférence de presse sera diffusée en direct sur Internet et sera accessible dans le site Web du Service de police de Vancouver à vpd.ca ou en cliquant sur conférence de presse en direct du SPV.

Pour de plus amples renseignements :

Agent Brian Montague
Relations avec les médias
Service de police de Vancouver
Tél. : 604-717-2807 – Courriel : brian.montague@vpd.ca

Timothy M. Smith
Relations gouvernementales et communications stratégiques
Association canadienne des chefs de police
Tél. : 613-601-0692 – Courriel : timsmith2000@rogers.com

L'Association canadienne des chefs de police (ACCP) a été fondée en 1905 et elle compte aujourd'hui plus de 1000 membres de toutes les régions du Canada. Par l'entremise de ses membres chefs de police et autres hauts dirigeants policiers, l'ACCP représente plus de 90 % du milieu policier au Canada, y compris aux échelons fédéral, provincial, régional et municipal, au sein des Premières Nations, dans les transports et dans les Forces canadiennes. L'ACCP a pour mission d'être « à l'avant-garde du progrès policier ».

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

COMMUNIQUÉ

POUR DIFFUSION IMMÉDIATE
Le 26 octobre 2012

La police confirme les cinq plus grandes craintes des Canadiens au sujet du projet de loi C-30

L'ACCP réitère son appel à l'action en faveur de mesures législatives sur l'accès légal

VANCOUVER (Colombie-Britannique) – L'Association canadienne des chefs de police (ACCP) renouvelle ses efforts en vue d'informer les Canadiens sur la question des pouvoirs policiers d'« accès légal » dans le contexte du projet de loi C-30 – la « *Loi sur la protection des enfants contre les cyberprédateurs* ».

« Si nous restons à rien faire, les criminels continueront d'exploiter les technologies modernes pour harceler et menacer, pour commettre des fraudes et des escroqueries, pour se livrer à des activités du crime organisé et pour commettre des violences sans guère craindre d'être arrêtés, a affirmé le président de l'ACCP le chef Jim Chu. Les Canadiens ont besoin de la même protection contre les criminels que dans d'autres démocraties occidentales. »

Des gouvernements canadiens précédents ont présenté des projets de loi sur l'accès légal, qui ont chaque fois fini par « mourir au Feuilleton ». L'ACCP n'est pas prête à voir le projet de loi C-30 subir le même sort.

« Si nous ne prenons pas une position ferme dans ce dossier, a poursuivi le chef Chu, les Canadiens n'apprécieront pas les restrictions imposées à l'application de la loi dans le cybermonde. L'application de la loi continue d'être entravée par une loi datant de 1975, à l'époque du téléphone à cadran. Aujourd'hui, nous permettons que de nouvelles technologies servent de refuge pour des activités criminelles graves, mais nous sommes réticents à utiliser la technologie pour prévenir ces crimes graves et faire enquête sur eux. »

« Si les lois des années 1970 ne sont pas modernisées, des criminels organisés planifieront leurs assassinats et enlèvements en utilisant les services de entreprises de télécommunication qui ne dotent pas leurs systèmes des moyens techniques voulus pour réunir des preuves. Des terroristes exploiteront ces mêmes lacunes. Des victimes d'escroqueries ou d'extorsion sur Internet découvriront que les traces

électroniques reliant un suspect au crime ont disparu parce que le fournisseur de services de télécommunication n'avait pas l'obligation légale de conserver les données. Si un suspect attire un enfant en utilisant un téléphone terrestre, les renseignements de base sur l'abonné se trouvent dans un bottin. Mais les prédateurs d'aujourd'hui n'utilisent pas la vieille technologie. Le parent d'un enfant qui a été leurré sur Internet apprendra que les recherches menées par la police pour retrouver leur enfant sont retardées parce qu'il faut d'abord un mandat pour obtenir les renseignements de base sur les abonnés. »

« L'intimidation criminelle est une grande source de préoccupation pour tous les Canadiens, surtout les parents de jeunes enfants, et le projet de loi C-30 contient aussi de nouvelles mesures législatives qui aideraient la police à intervenir et faire enquête rapidement en cas de cyberintimidation, et ainsi éviter des tragédies inutiles. Le projet de loi érige en infraction le fait d'utiliser les télécommunications, y compris les médias sociaux et Internet, pour nuire à une personne, l'alarmer ou la harceler. »

Il faut que les Canadiens comprennent ce qu'est véritablement l'accès légal.

L'ACCP a produit une vidéo intitulée « La police confirme les 5 plus grandes craintes des Canadiens au sujet du projet de loi C-30 », qu'on peut voir à http://youtu.be/w5U1_LsUBeU. En outre, pour susciter une discussion éclairée à ce sujet, l'ACCP a rédigé un document intitulé « Simplifier l'accès légal – Dans l'optique de l'application de la loi ». Il se trouve dans le site Web de l'ACCP (www.CACP.ca), ou directement à http://www.cacp.ca/media/library/download/1244/f_Simplifying_Lawful_Access.pdf Le document compare l'environnement d'aujourd'hui à celui que créeraient les nouvelles mesures législatives proposées, il répond aux questions les plus fréquentes et il comprend une série d'études de cas décrivant la façon dont les responsables de l'application de la loi utilisent les renseignements de base sur les abonnés.

L'ACCP appuie le projet de loi C-30, mais tient à préciser qu'elle partage les préoccupations que certains ont exprimées au sujet d'une partie du projet de loi. La formulation actuelle de l'article 34 donne à croire qu'un inspecteur peut perquisitionner toute chose, y compris les renseignements privés des Canadiens se trouvant dans des installations de télécommunication, pour vérifier la conformité à la Loi. On comprend aisément comment cette formulation mènerait à la supposition que les inspecteurs pourraient accéder librement aux dossiers personnels des Canadiens au cours de ces inspections. Bien que nous comprenions que telle n'est pas l'intention de cet article, il y aurait lieu de le clarifier. Nous reconnaissons que de telles inspections sont nécessaires, mais la formulation de l'article 34 doit être modifiée pour rassurer les Canadiens que leurs renseignements personnels ne seront jamais visés par cette inspection.

L'ACCP incite nos élus à doter la police d'outils modernes pour qu'elle puisse mieux protéger les Canadiens. C'est ce que ferait le projet de loi C-30. L'ACCP est d'accord avec les dispositions du projet de loi C-30 renforçant la reddition de comptes et la surveillance pour protéger le public contre la mauvaise utilisation des pouvoirs d'interception de la police.

L'ACCP incite les députés, les médias et tous les Canadiens à considérer l'importance de ce projet de loi en tenant compte des victimes de la criminalité d'aujourd'hui, et en pensant aux agents d'application de la loi de première ligne qui tentent de prévenir les crimes et font enquête sur les crimes.

L'Association canadienne des chefs de police a été fondée en 1905 et elle représente quelque 1000 dirigeants policiers de toutes les régions du Canada. Elle s'emploie à appuyer et promouvoir l'efficacité dans l'application de la loi ainsi que la protection et la sécurité de la population du Canada. Par l'entremise de ses membres chefs de police et autres hauts dirigeants policiers, l'ACCP représente plus de 90 % du milieu policier au Canada, y compris aux échelons fédéral, provincial, régional et municipal, au sein des Premières Nations, dans les transports et dans les Forces canadiennes.

Pour de plus amples renseignements :

Timothy M. Smith
Relations gouvernementales et communications
Association canadienne des chefs de police
Tél. : 613-601-0692
Courriel : timsmith2000@rogers.com

Simplifier l'accès légal – Projet de loi C-30 – Dans l'optique de l'application de la loi

Introduction

Lorsque les intervenants en application de la loi utilisent des termes tels qu'écoute électronique, capacité d'interception ou surveillance électronique et lorsqu'ils évoquent en même temps les moyens de communication les plus répandus – Internet, téléphone cellulaire, médias sociaux –, il est compréhensible que de nombreux Canadiens s'inquiètent. C'est au point où la plupart d'entre nous, dans le milieu de l'application de la loi, serions d'accord avec cette opinion soulignée par la commissaire à la vie privée du Canada à l'issue d'un sondage auprès des Canadiens : « Plus de huit répondants sur dix (82 %) s'opposent à ce que les services policiers et les agences de renseignements aient accès à leurs dossiers de courriel et à d'autres données concernant la façon dont ils utilisent Internet sans avoir obtenu un mandat d'un tribunal. » Mais ce n'est pas vraiment ce que proposent les gouvernements et les responsables de l'application de la loi au Canada.

Ces mêmes technologies permettent de se livrer à de graves activités criminelles au Canada – ce dont profitent par exemple le crime organisé, les prédateurs sexuels, les gangs, les voleurs d'identité et les terroristes. Les nouvelles technologies offrent de nouvelles façons de commettre des crimes anciens et ont engendré de nouveaux crimes – dont la diffusion de virus, chevaux de Troie, vers, logiciels espions et pourriel, le piratage informatique, le hameçonnage, le vol d'identité, la fraude sur Internet et le blanchiment d'argent. Le régime législatif désuet du Canada date de 1975, à l'époque du téléphone à cadran. Il est devenu urgent de moderniser les dispositions législatives pour tenir compte des grands progrès des technologies des communications. En attendant, le cadre législatif actuel pose de grandes difficultés dans les enquêtes policières et compromet la sécurité publique. Des modifications immédiates s'imposent pour permettre à la police de faire enquête légalement et efficacement sur de graves infractions. Les modifications proposées visent à actualiser les lois pour tenir compte des nouvelles technologies.

Nous croyons que les nouvelles mesures législatives :

- aideront la police en lui apportant les outils voulus pour faire enquête sur les crimes tout en tenant compte des droits des Canadiens à la vie privée – voire en les renforçant en ajoutant des moyens de contrôle qui n'existent pas actuellement;
- aideront les responsables de l'application de la loi à appréhender ceux qui se livrent à ces activités criminelles en utilisant les nouvelles technologies pour échapper à l'appréhension en raison de lois et de technologies dépassées;
- permettront d'accéder rapidement et sûrement à des renseignements de base utiles aux enquêtes policières et à d'autres fonctions qu'assure la police au service du public (p. ex., prévention du suicide, communication avec les proches parents d'une victime, etc.).

Une des difficultés au sujet des mesures législatives sur l'accès légal est de les présenter d'une façon compréhensible pour le public, étant entendu qu'elles peuvent être très techniques. Notre but est d'aider le public à s'en faire une opinion sur la base de faits et non de rhétorique.

L'environnement actuel et les dispositions législatives proposées

Il existe actuellement peu de modalités précises auxquelles les responsables de l'application de la loi peuvent recourir pour obtenir l'information requise afin de faire enquête sur des pistes ayant trait à des activités criminelles. Les fournisseurs de services de télécommunication (FST ou télécommunicateurs) communiquent aux responsables de l'application de la loi des renseignements très différents d'un cas à l'autre. Le tableau suivant décrit la façon dont le projet de loi C-30 resserre les règles par rapport à la situation actuelle dans différentes circonstances.

Objet	Situation actuelle	Effet du projet de loi C-30
- Obtention du contenu d'un courriel, d'un appel cellulaire, etc.	Uniquement en vertu d'un mandat*	Uniquement en vertu d'un mandat*
- Obtention de renseignements de base sur les abonnés dans le cadre d'activités de sécurité publique	Au cas par cas – Certains télécommunicateurs communiquent les renseignements, de nombreux autres exigent un mandat. Le problème est d'assurer la rapidité et l'uniformité de l'accès aux renseignements. Aucun moyen de contrôle n'existe à l'égard de l'obtention de renseignements.	- Strictes limites quant au nombre de responsables de l'application de la loi autorisés à demander des renseignements - Ces responsables recevront une formation complète. - Strictes modalités prévues pour la consignation des demandes de renseignements, la production de rapports et la vérification. - Exigences de vérification / production de rapports comprenant la transmission de documents au ministre de la Sécurité publique, au commissaire à la protection de la vie privée, aux autorités provinciales, etc.
- Adresse IP ou localisation cellulaire (surveillance)	- Uniquement en vertu d'un mandat	- Uniquement en vertu d'un mandat
- Surveillance de la navigation sur Internet	- Uniquement en vertu d'un mandat	- Uniquement en vertu d'un mandat

Objet	Situation actuelle	Effet du projet de loi C-30
- Mécanisme d'obtention du contenu d'un courriel, d'un appel cellulaire, etc.	- Uniquement en vertu d'un mandat* Au cas par cas – Les télécommunicateurs ne sont pas tenus de conserver les données. Avant que les responsables de l'application de la loi n'obtiennent un mandat, le contenu peut avoir disparu. La situation handicape gravement la capacité d'action des responsables de l'application de la loi et peut mettre des vies en danger.	- Uniquement en vertu d'un mandat* - Prévoit des ordonnances de production et des ordonnances de préservation** - Permet aux responsables de l'application de la loi de demander à un télécommunicateur de préserver des données pendant qu'ils demandent un mandat (aide à éviter que les données soient perdues)

* Un mandat est une autorisation judiciaire permettant aux responsables de l'application de la loi d'obtenir des renseignements privées (contenu ou données). Il existe certaines situations d'urgence (p. ex., danger de mort immédiat) où les responsables de l'application de la loi peuvent obtenir ces renseignements. Le projet de loi C-30 n'y change rien.

** Ce projet de loi crée des ordonnances de communication et de préservation ainsi que des ordres de préservation que la police peut présenter à un télécommunicateur. Une ordonnance de communication permet à la police d'obtenir l'accès à une quantité limitée de données de transmission dans le but ultime d'identifier le fournisseur de services qui est à l'origine de la transmission de courriels ou autres communications. Elle serait accordée sous forme de mandat sur la foi de « motifs raisonnables de soupçonner ». Un ordre de préservation exige qu'un télécommunicateur préserve (c.-à-d., n'efface pas) des données informatiques ou données de communication précises qui seraient utiles à une enquête; l'ordre porte sur une période maximale de 21 jours (90 jours dans le cas d'enquêtes sur des infractions à des lois étrangères), tandis que la police demande un mandat lui permettant d'accéder aux données en cause.

Les faits importants au sujet des mesures législatives

Accès aux données ou au contenu

Fait : Pour obtenir le contenu de communications électroniques, un mandat est requis. Des données ou le contenu de transmissions peuvent uniquement être communiqués aux organismes d'application de la loi dans le cadre d'un processus de mandats délivrés par un tribunal. Le projet de loi n'y change rien. (Il y a seulement des exceptions très limitées en cas de situation d'urgence où un grave préjudice doit être évité.)

L'« ordre de préservation de données » présenté par un organisme policier oblige un fournisseur de services de télécommunication à préserver des données pendant une période maximale de 21 jours (pour donner à la police le temps de demander le mandat voulu afin d'obtenir l'information en cause). Le fournisseur de services doit conserver les données existantes en lieu sûr en attendant qu'un mandat soit délivré.

Fait : Le projet de loi ne demande pas que le fournisseur de services surveille les communications de la personne visée ou fasse rapport à l'organisme d'application de la loi sur l'activité d'une personne (il ne s'agit pas d'une « ordonnance de collecte »).

Accès aux renseignements de base sur les abonnés

Les renseignements que les entreprises seraient obligées de communiquer sont : nom, adresse, numéro de téléphone, adresse de courriel, adresse IP et nom du fournisseur de services. Dans tous les cas, la police fournirait un identificateur (p. ex., adresse IP et heure / date), et le fournisseur de services de communication communiquerait les renseignements de l'abonné correspondant (p. ex., nom du client). Bien que ces renseignements soient importants pour la police dans tous genres d'enquêtes, ils peuvent revêtir une importance vitale lorsqu'il est urgent que la police localise une personne qui appelle ou qui est à l'origine de renseignements donnant à la police des motifs raisonnables de soupçonner qu'une personne est en danger. Sans ces renseignements, la police peut être incapable de localiser rapidement une personne qui est en difficulté ou qui est victimisée et lui venir à l'aide.

Fait : Les renseignements de base sur les abonnés (nom, adresse, numéro de téléphone, etc.) pourraient être obtenus en vertu de demandes présentées par une personne désignée au sein d'un organisme policier, dans le cadre d'un processus vérifié. Cette possibilité tient compte de la réalité qu'il n'existe pas nécessairement de bottins de téléphone dans le monde numérique.

Le processus de vérification

Actuellement, il n'existe aucun processus vérifié permettant aux responsables de l'application de la loi d'obtenir l'accès aux renseignements de base sur un abonné. Les renseignements peuvent être obtenus du fait d'une relation existante entre un service de police et un télécommunicateur, ou, trop souvent, ils sont fournis seulement après de longs délais. Certains télécommunicateurs refusent tout simplement de communiquer les renseignements sans un mandat. *Actuellement, les organismes d'application de la loi ne sont pas tenus de rendre des comptes au sujet de ces demandes ou des renseignements qu'ils obtiennent.*

Fait : En vertu du projet de loi, de nouveaux moyens de protection augmenteront en fait la protection de la vie privée des Canadiens. En font partie :

- *de strictes limites sur le nombre de responsables de l'application de la loi qui sont autorisés à demander des renseignements;*
- *la formation de ces personnes;*
- *des modalités strictes quant à la consignation de ces demandes, la production de rapports et la vérification;*
- *la mise en œuvre d'un processus de vérification / production de rapports comprenant la transmission de documents au ministre de la Sécurité publique, au commissaire à la protection de la vie privée, à diverses autorités fédérales et provinciales, etc.*

Conformité de la part des télécommunicateurs et FSI

Certains ont soutenu que l'interception des communications est un problème en raison du coût prohibitif des modifications nécessaires de la part des fournisseurs de services existants confrontés à l'arrivée de nouveaux concurrents sur le marché.

Fait : Dans ce projet de loi, le gouvernement reconnaît le coût de développement de l'équipement des fournisseurs et est disposé à apporter une aide dans des circonstances précises. Il y a des dispositions protégeant les fournisseurs existants et leur accordant une période d'adaptation, avec une possibilité d'aide financière de la part du gouvernement.

Autre

Localisation de téléphones (dotés d'une capacité GPS) en l'absence d'un mandat. Une telle possibilité existe déjà en vertu du *Code criminel* (article 487.11), mais uniquement en situation d'urgence (p. ex., kidnapping ou extorsion). Ce même article (légèrement révisé pour englober un enregistreur de numéros) subsistera dans les nouvelles mesures législatives.

Questions fréquemment posées au sujet de l'accès légal

Q1

Pourquoi la police a-t-elle besoin d'un accès sans mandat aux renseignements de base sur les abonnés (p. ex., nom, adresse, services, données du compte)?

R1

- *Les renseignements de base sur l'abonné sont souvent les renseignements les plus élémentaires nécessaires pour faire progresser une enquête qui exigera éventuellement d'obtenir un mandat. Ils relèvent de la même logique que la recherche du nom d'une personne en fonction d'un numéro de téléphone figurant dans un carnet d'adresses. Le manque d'accès rapide à de tels renseignements peut bloquer des enquêtes, et le fait souvent. Dans une situation d'urgence, comme une information signalant un risque de suicide, des vies peuvent être mises en danger.*

- *Il existe actuellement peu de modalités auxquelles les responsables de l'application de la loi peuvent recourir pour obtenir l'information requise afin de faire enquête sur des pistes ayant trait à des activités criminelles. Les fournisseurs de services de télécommunication (FST ou télécommunicateurs) communiquent aux responsables de l'application de la loi des renseignements très différents d'un cas à l'autre. Les nouvelles mesures législatives :*

    - *aideront la police en lui apportant les outils voulus pour faire enquête sur les crimes tout en tenant compte des droits des Canadiens à la vie privée;*
    - *aideront les responsables de l'application de la loi à appréhender ceux qui commettent des crimes graves et qui échappent à l'appréhension en raison de lois et de technologies dépassées;*
    - *permettront d'accéder rapidement et sûrement à des renseignements de base utiles aux enquêtes sur des activités criminelles.*

- *Vers la fin du présent document, une section intitulée « Études de cas : L'utilité des renseignements de base sur les abonnés pour l'application de la loi » présente des exemples des raisons pour lesquelles la police a besoin de l'accès aux renseignements de base sur les abonnés. Pour illustrer la problématique, le Centre national de coordination contre l'exploitation des enfants de la GRC indique qu'en 2010, le délai moyen des réponses aux demandes de renseignements de base sur les abonnés était de 12 jours, et les renseignements ont été obtenus dans seulement 72,5 % des cas.*

- *Autres situations :*
    - *Déterminer l'adresse d'un témoin qui a donné son ou ses numéros de téléphone.*
    - *Suivre des pistes dans une enquête où elle a reçu un numéro de téléphone et doit :*
        - *déterminer s'il appartient à la personne à laquelle il est censé appartenir;*
        - *déterminer l'adresse à laquelle la personne habite (s'il s'agit d'un numéro de téléphone terrestre, puisque les adresses associées aux numéros de téléphone cellulaire ne sont guère fiables).*
    - *Obtenir l'information nécessaire à l'obtention d'un mandat (nom du client, adresse, adresse IP, numéro de téléphone, etc.).*
    - *Dans une situation d'urgence, par exemple un appel au 9-1-1 à partir d'un téléphone cellulaire ou un semblable appel à l'aide sur Internet. Les renseignements peuvent être essentiels en vue de venir en aide à une personne aussi rapidement que possible.*
    - *Faire diligence dans les enquêtes sur des affaires graves exigeant une intervention policière rapide afin d'appréhender des criminels ou prévenir un crime.*
    - *Informer les proches en cas d'accident ou d'homicide.*
    - *Informer le propriétaire de biens volés que les biens ont été retrouvés.*

Q1 (A)

Pourquoi la police ne peut-elle pas simplement obtenir un mandat pour les renseignements de base sur les abonnés?

R1 (A)

- *Le délai d'obtention d'un mandat ne permet pas nécessairement d'intervenir en temps utile, et peut mettre en jeu des vies et la sécurité. Dans de nombreux cas, la rapidité d'action est essentielle.*
- *La victimisation risque de se poursuivre pendant que la police demande un mandat.*
- *Dans de nombreux cas, les responsables de l'application de la loi ne peuvent pas obtenir un mandat sans les renseignements de base sur les abonnés en cause.*
- *Comment les responsables de l'application de la loi peuvent-ils obtenir en temps utile un mandat en cas de menaces de suicide ou en vue de communiquer avec les proches parents d'une victime?*
- *Dans les cas de personnes disparues, la police n'a souvent pas de motifs évidents pour conclure qu'un crime est en cause ou qu'il y a urgence. Il peut être impossible d'obtenir un mandat, et les fournisseurs de services de télécommunication ne sont pas tenus de communiquer les renseignements de base sur les abonnés. Dans ces cas, les premières 24 heures d'une enquête sont vitales.*
- *Les renseignements de base sur les abonnés permettent de faire enquête rapidement, sur la base d'une intrusion minimale (coordonnées) dans la vie des gens.*
- *Si un mandat était nécessaire pour chaque demande de renseignements de base sur les abonnés, les policiers (et les juges) ne pourraient pas satisfaire à la demande. En outre, la complexité des affaires touchant plus d'un ressort (à l'échelle provinciale, nationale ou internationale) imposerait une importante charge de travail aux autorités policières en vue d'obtenir un mandat à chaque endroit pertinent.*
- *Il faut noter que la notion d'urgence peut être subjective. Les mesures législatives proposées assurent un cadre uniformisé pour l'obtention de tels renseignements.*

- *Encore une fois, dans le contexte d'aujourd'hui, les télécommunicateurs peuvent communiquer des renseignements de base sur les abonnés à titre volontaire quelles que soient les pratiques de télécommunicateurs individuels. Ce projet de loi prévoit une surveillance qui est actuellement absente. Les autorités d'application de la loi souhaitent un cadre uniformisé où les télécommunicateurs ne sont pas ceux qui décident de façon aléatoire quelles enquêtes elles peuvent ou non mener.*

Q2

Qui peut demander les renseignements de base sur les abonnés aux fournisseurs de services?

R2

Actuellement tout agent assermenté ou employé civil d'un corps policier peut demander ces renseignements à une entreprise de télécommunications. Les nouvelles dispositions exigeront que le dirigeant d'un organisme d'application de la loi (p. ex., chef ou commissaire) désigne dans son organisation un nombre limité de personnes habilitées à demander ces renseignements. Toutes les personnes désignées devront recevoir une formation. Les organismes d'application de la loi devront consigner toutes les demandes et les déclarer dans le cadre d'un processus de vérification prévu par le projet de loi. Le processus de vérification comprend :

- *de strictes limites quant au nombre de responsables de l'application de la loi autorisés à demander des renseignements;*
- *la formation de ces responsables;*
- *de strictes modalités pour la consignation des demandes de renseignements, la production de rapports et la vérification;*
- *la mise en place d'un processus de vérification / production de rapports comprenant la transmission de documents au ministre de la Sécurité publique, au commissaire à la protection de la vie privée, à diverses autorités fédérales et autorités provinciales, etc.*

Q3

À quoi serviront les renseignements de base sur les abonnés obtenus par le personnel d'application de la loi auprès des fournisseurs de services?

R3

Ces renseignements sont fournis au personnel policier aux fins d'enquêtes et à des fins de sécurité publique.

- *Il existe actuellement une règle acceptée voulant que les renseignements obtenus puissent seulement servir aux fins pour lesquelles ils ont été obtenus. Aucune instance ne le vérifie actuellement, et il n'y a aucune exigence faite aux organismes d'application de la loi de rendre des comptes sur les fins pour lesquelles des renseignements ont été obtenus et les fins pour lesquelles ils ont été utilisés.*

- *Les nouvelles dispositions garantissent que :*
    - *les organismes d'application de la loi puissent expliquer la raison pour laquelle des renseignements ont été obtenus et les fins auxquelles ils ont servi;*
    - *un organisme puisse utiliser des renseignements uniquement aux fins pour lesquelles ils ont été obtenus;*
    - *un organisme classe les renseignements de façon à permettre une vérification visant à déterminer pourquoi ils ont été demandés et à quelles fins ils ont servi.*

Q4

Les organismes d'application de la loi font-ils actuellement de l'interception de communications sans mandat ou autorisation judiciaire?

R4

Depuis 1993, l'article 184.4 du Code criminel *prévoit qu'un agent de la paix peut intercepter une communication privée sans autorisation judiciaire (i) s'il a des motifs raisonnables de croire qu'une autorisation ne peut pas être obtenue avec toute la diligence raisonnable voulue dans les circonstances; (ii) s'il a des motifs raisonnables de croire qu'une interception immédiate est nécessaire pour empêcher un acte illicite qui causerait des dommages sérieux à une personne ou un bien; et (iii) si l'auteur ou le destinataire de la communication est soit la personne qui commettrait l'acte en cause ou la personne visée par l'acte.*

En 2008, la constitutionnalité de cet article a été contestée dans l'affaire R. v. Six Accused Persons *(en instance à la Cour suprême). La loi, dans sa forme actuelle, n'exige pas de déclarer le recours à cet article au procureur général (provincial) ou à Sécurité publique Canada (au fédéral). En outre, au contraire des interceptions approuvées par un juge, il n'y a nulle obligation d'informer la ou les personnes visées par l'interception. L'ancien projet de loi C-50 visait à modifier la loi actuelle pour pallier ces deux lacunes.*

Q5

Les nouvelles dispositions habiliteront-elles réellement les fournisseurs de services Internet (FSI) à recueillir des renseignements et à les communiquer aux organismes d'application de la loi sans mandat?

R5

Absolument pas. Un organisme d'application de la loi sera habilité à présenter un « ordre » de préservation des données pendant 21 jours. Le fournisseur de services préservera les renseignements pendant cette période mais l'organisme d'application de la loi DEVRA avoir un mandat pour obtenir les données visées par la demande (ou obtenir une ordonnance d'un tribunal exigeant la préservation des données pendant 90 jours de plus).

Q6

Les nouvelles dispositions n'handicaperont-elles pas financièrement les fournisseurs de services de télécommunication et fournisseurs de services Internet compte tenu de toutes les nouvelles exigences en matière de capacité d'interception?

R6

Cette question a été prise en compte dans la rédaction des dispositions. Dans ce projet de loi, le gouvernement reconnaît le coût de développement de l'équipement des fournisseurs et est disposé à apporter une aide dans des circonstances précises. Il y a des dispositions protégeant les fournisseurs existants et leur accordant une période d'adaptation, avec une possibilité d'aide financière de la part du gouvernement. Il faut noter que des lois d'une bien plus grande portée existent aux États-Unis et en Europe, où les télécommunicateurs (pour des raisons dè concurrence) n'ont pas transmis les coûts aux consommateurs.

Q7

Alors que certains d'entre nous passons notre vie en ligne et supposons qu'il y a un certain anonymat dans ce domaine, ces mesures législatives ne confèrent-elles pas à « l'État » la capacité de surveiller ce que nous faisons et de recueillir des renseignements sur nous sans raison valable?

R7

Absolument pas. Ces mesures législatives ne sont pas destinées à supprimer la nécessité d'un mandat pour obtenir des renseignements qui exigent actuellement un mandat. Elles visent à moderniser le Code criminel *selon la réalité de ce siècle et de cette décennie et à permettre la préservation de données qui pourraient autrement ne pas être conservées, afin de donner aux organismes d'application de la loi le temps de demander un mandat pour pouvoir obtenir ces renseignements. Les crimes commis en utilisant les services et les sites disponibles sur Internet sont en hausse – depuis l'exploitation des enfants jusqu'au vol d'identité –, et les organismes d'application de la loi ont besoin de la capacité d'obtenir les données voulues pour déterminer si une personne soupçonnée a commis un crime. Ces renseignements pourraient être obtenus seulement si un juge a délivré un mandat à cette fin.*

Les dispositions sur les renseignements de base des abonnés ne confèrent pas aux responsables de l'application de la loi le pouvoir légal de surveiller des sites Web en vue de dresser des profils de particuliers ou de localiser des particuliers. En vertu du projet de loi, la police peut demander le nom et l'adresse associés à une adresse IP, par la voie d'une demande de renseignements de base sur l'abonné.

Les demandes de renseignements adressées à un fournisseur des services de télécommunication au sujet de l'activité de navigation sur Internet ou de la localisation en temps réel d'une personne devraient être présentées en vertu d'une ordonnance de communication, d'un mandat ou d'une autorisation d'écoute électronique que prévoit le Code criminel.

Q8

J'ai entendu dire que les entreprises de télécommunications et les FSI suivront mes déplacements par mon téléphone ou mon utilisation d'Internet, et transmettront les renseignements aux organismes d'application de la loi. Est-ce vrai?

R8

Actuellement et tout autant selon les nouvelles dispositions, c'est seulement si un mandat a été délivré ou en cas de situation d'urgence que les entreprises de télécommunications et les FSI communiquent ces renseignements à des organismes d'application de la loi. Un mandat sera toujours nécessaire pour obtenir ces renseignements à moins qu'un organisme d'application de la loi invoque soit l'article 487.11, l'article 184.4 ou l'article 492.1 du Code criminel. *Les modifications qu'apportent les nouvelles mesures législatives introduisent de nouvelles protections de la vie privée et des droits garantis par la Charte, et exigent que les fournisseurs de services aient la capacité de fournir les renseignements.*

Q9

Ces mesures législatives ne sont-elles pas simplement une tentative du gouvernement et de la police de faire en sorte que « l'État » dispose d'yeux et d'oreilles partout et puisse violer la vie privée sans raison valable?

A9

Les mesures législatives visent à obliger les fournisseurs de services à disposer de la capacité d'intercepter des communications privées conformément à une ordonnance d'un tribunal ou en cas de situation d'urgence. Elles précisent aussi que les renseignements de base sur les abonnés doivent être communiqués à des agents d'application de la loi sans mandat (alors qu'aucune loi ne l'exige actuellement), mais clarifie les règles que doivent suivre aussi bien la police que le fournisseur de services. Par exemple, comme un fournisseur de services serait tenu de communiquer des renseignements sur demande, les organismes d'application de la loi sont maintenant tenus de prévoir des moyens de vérifier clairement les raisons pour lesquelles des renseignements ont été demandés et les fins auxquelles ils ont été utilisés (ce qui n'est pas actuellement exigé).

L'ombudsman fédéral des victimes d'actes criminels et la nécessité de l'accès légal

Le Bureau de l'ombudsman fédéral des victimes d'actes criminels est une ressource indépendante pour les victimes au Canada. Il a été créé en 2007 afin de veiller à ce que le gouvernement du Canada s'acquitte de ses responsabilités à l'égard des victimes d'actes criminels. M^me^ Sue O'Sullivan est l'ombudsman fédéral des victimes d'actes criminels. Tout comme son prédécesseur, elle a étayé la nécessité de l'accès légal.

L'ombudsman a fait valoir au Parlement l'importance du problème de l'exploitation sexuelle des enfants et la nécessité de l'accès légal. Dans son rapport *Chaque image, chaque enfant – L'exploitation sexuelle d'enfants facilitée par Internet au Canada*, l'ombudsman décrit les très grands problèmes auxquels sont confrontés les responsables de l'application de la loi. Lorsqu'elle a comparu devant un comité sénatorial au sujet du projet de loi C-22 (*Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet*), elle s'est exprimée comme suit :

> *Malgré notre appui ferme à ce projet de loi, je dois souligner qu'il reste encore beaucoup à faire pour combattre efficacement le problème de l'exploitation sexuelle d'enfants facilitée par Internet. Le projet de loi C-22 n'empêchera pas à lui seul la production ni la communication du matériel d'exploitation sexuelle d'enfants. Il ne réglera pas non plus les problèmes que connaissent les autorités policières pour enquêter sur les affaires de ce genre sans pouvoir obliger, sans autorité, les fournisseurs de services Internet à leur communiquer le nom et l'adresse des clients afin de leur permettre d'identifier les personnes associées à une adresse IP particulière.*
>
> *À l'heure actuelle, les fournisseurs de services Internet sont autorisés à communiquer sans mandat le nom et l'adresse du client, mais ils ne sont pas obligés de le faire. Même si de nombreuses compagnies acceptent de collaborer avec la police, certaines peuvent refuser, et refusent de le faire. En fait, selon un mémoire soumis par le Centre national de coordination contre l'exploitation des enfants en 2007, de 30 à 40 p. 100 des demandes sont rejetées. Si elles ne peuvent obtenir ces renseignements, les autorités policières devront fermer certains dossiers avant même d'avoir entrepris une enquête détaillée.*
>
> *Quand il est question de la protection de la vie privée, celle de la victime doit avoir préséance. Je ne pense pas qu'il y ait quoi que ce soit qui porte plus atteinte à votre vie privée que de voir circuler votre agression sexuelle dans le cyberespace. C'est une question d'équilibre et de respect du droit à la vie privée des victimes d'agression sexuelle.*

Pour de plus amples renseignements :

- Comparution du 10 février 2011 de M^me^ O'Sullivan devant le Comité sénatorial permanent des affaires juridiques et constitutionnelles, au sujet du projet de loi C-22 : www.parl.gc.ca/Content/SEN/Committee/403/lega/20evb-f.htm?Language=E&Parl=40&Ses=3&comm_id=11
- Rapport *Chaque image, chaque enfant* : www.victimesdabord.gc.ca/res/pub/pjuvenile-childp/cont_01.html
- Document d'information – *Chaque image, chaque enfant* : www.victimesdabord.gc.ca/media/nouv-news/di-bg/20090507-1.html

- Faits en bref et statistiques – *Chaque image, chaque enfant* : www.victimesdabord.gc.ca/media/nouv-news/di-bg/20090507-2.html

Études de cas : L'utilité des renseignements de base sur les abonnés pour l'application de la loi

Un des problèmes du système actuel est qu'il n'y a ni uniformité ni assurances quant à la façon dont les télécommunicateurs répondent, quand ils le font, aux demandes de renseignements de base sur des abonnés. Par exemple :

- un certain télécommunicateur ne répond aux demandes de renseignements de base sur des abonnés que le vendredi, peu importe quand elles sont présentées;
- un certain télécommunicateur n'accepte les demandes de renseignements de base sur des abonnés que par courriel.

Le Centre national de coordination contre l'exploitation des enfants, à Ottawa, a examiné 1244 demandes de renseignements de base des abonnés qu'il a présentées en 2010. Les fournisseurs de services ont communiqué les renseignements dans 902 cas (72,5 %). Par contre dans 62 cas (5 %), les fournisseurs de services ont refusé de les communiquer sans mandat judiciaire; dans 53 cas (4,3 %), ils n'ont pas répondu à la demande. Dans 227 cas, (18,2 %), les fournisseurs de services ne possédaient pas les renseignements que les autorités demandaient. Ces chiffres ne comprennent pas les demandes présentées par d'autres unités qui font enquête sur des infractions liées à l'exploitation sexuelle des enfants sur Internet, partout au pays.

Par ailleurs en 2010, le délai moyen de réponse aux demandes était de 12 jours.

Le Centre national de coordination contre l'exploitation des enfants, à Ottawa, a indiqué que sur les 482 demandes de renseignements de base des abonnés qu'il a présentées en 2007, les fournisseurs de services ont dans 19 cas (3,9 %) refusé de communiquer les renseignements sans mandat judiciaire; dans 92 cas (19,1 %), ils n'ont pas répondu à la demande. Dans 40 cas (8,3 %), les fournisseurs de services ne possédaient pas les renseignements demandés. En 2008, le Centre national de coordination contre l'exploitation des enfants, à Ottawa, a présenté 335 demandes de renseignements de base des abonnés. Les fournisseurs de services ont dans 6 cas (1,8 %) refusé communiquer les renseignements sans mandat judiciaire; dans 46 cas (13,7 %), ils n'ont pas répondu à la demande. Dans 30 cas (9 %), les fournisseurs de services ne possédaient pas les renseignements demandés.

Exemples de la disparité régionale dans la communication de renseignements de base sur les abonnés par les télécommunicateurs

Les télécommunicateurs de certaines régions ne répondent parfois pas aux demandes. Certains télécommunicateurs du Canada atlantique ne communiquent pas de renseignements de base sur les abonnés sans mandat.

1) En décembre 2010, la GRC au Nouveau-Brunswick a entamé une enquête sur une affaire d'échange entre pairs de pornographie juvénile. La police soupçonnait que 170 adresses IP étaient associées à une seule personne. Ces adresses IP appartenaient à un télécommunicateur réputé être opposé à la communication volontaire de renseignements sur les abonnés sans mandat, donc la police a demandé un mandat.

En conséquence, les renseignements de base sur les abonnés ont été communiqués 15 jours plus tard, alors que l'activité Internet du suspect avait cessé. En septembre 2011, le suspect a repris son activité en ligne. Cette fois, le télécommunicateur a communiqué les renseignements de base sur l'abonné de façon volontaire. Cette coopération a permis à la police d'agir rapidement et d'arrêter le suspect à son domicile en octobre 2011. Le suspect a été accusé de possession et distribution de pornographie juvénile. En outre, la police a découvert qu'il produisait de la pornographie juvénile, et il a aussi été accusé de ce crime. Le suspect a aussi plaidé coupable à des accusations d'abus à l'égard de deux garçons au Nouveau-Brunswick. Si la police avait pu obtenir les renseignements au début de son enquête, elle aurait pu procéder plus rapidement à l'arrestation, et mettre fin plus tôt aux abus sexuels perpétrés par le suspect.

<u>Exemples de cas où des télécommunicateurs n'ont pas communiqué des renseignements de base sur les abonnés à la police</u>

2) En 2007, 88 adresses IP canadiennes ont été mises en cause dans une affaire internationale de pornographie juvénile. La police a demandé les renseignements de base sur les abonnés associés à ces adresses. Dans 51 cas, les renseignements ont été communiqués et la police a pu faire enquête sur les personnes en cause et porter certaines accusations. Par contre 37 demandes sont restées sans réponse de la part des fournisseurs de services. Par conséquent, l'identité et la localisation des pédophiles soupçonnés restent inconnues.

3) En 2008 dans l'Opération Koala, une affaire internationale majeure de pornographie juvénile, Europol a communiqué à la GRC des renseignements ayant trait à 98 comptes de courriel ou adresses IP au Canada. Les télécommunicateurs ont été priés de communiquer les renseignements de base sur les abonnés en cause. De nombreux fournisseurs de services ont communiqué les renseignements de base, ce qui a mené à l'arrestation et la poursuite de neuf Canadiens. Malheureusement, l'identité des détenteurs de 25 adresses IP ou comptes de courriel n'a pas pu être établie faute de coopération de la part de certains fournisseurs de services.

4) Dans une enquête internationale sur la pornographie juvénile, les télécommunicateurs ont refusé de faire suite à 47 des 200 demandes de renseignements de base sur les abonnés qui leur ont été présentées.

5) En 2007, la GRC a participé à une enquête internationale dans laquelle certains suspects se trouvant au Canada tentaient de frauder des entreprises américaines à hauteur de 100 millions de dollars. L'enquête exigeait que la police trouve les personnes qui accédaient à des réseaux informatiques non sécurisés dans la région de Toronto (piratage Wi-Fi) afin de commettre ces activités frauduleuses. Les suspects se déplaçaient sans cesse et la police avait besoin de la coopération immédiate des télécommunicateurs pour localiser ces réseaux. Cependant, les télécommunicateurs n'ont pas voulu communiquer à la police les renseignements de base sur les abonnés dont elle avait besoin. Par conséquent, il a fallu cinq jours complets de travail de huit enquêteurs techniques pour localiser et arrêter les suspects. Les suspects ont réussi à dérober 15 millions de dollars aux victimes. Si la police avait reçu les renseignements quand elle les a demandés, la valeur de la fraude aurait été sensiblement moindre, et les ressources policières auraient pu être utilisées plus efficacement.

6) En 2009, une enquête criminelle internationale a mis en cause 78 adresses IP canadiennes associées à l'achat de pornographie juvénile. Des demandes de renseignements de base sur les abonnés ont été présentées aux télécommunicateurs pertinents, lesquels ont communiqué les

renseignements à l'égard de 44 adresses. Cependant, 18 suspects n'ont pas pu être identifiés parce que les fournisseurs de services ont refusé de communiquer les renseignements de base sur les abonnés aux autorités à moins qu'elles n'obtiennent d'abord un mandat.

7) En 2009, la GRC en Alberta a été prévenue d'une menace de tuerie scolaire proférée en ligne. La police possédait l'adresse IP utilisée ainsi que la date et l'heure où la menace avait été proférée, et elle a demandé au télécommunicateur de lui communiquer les données de base sur l'abonné correspondant. Le télécommunicateur a refusé, estimant qu'il n'y avait pas urgence puisque la menace datait de six jours. Le lendemain (un vendredi avant une longue fin de semaine), la police a demandé une ordonnance de communication visant à contraindre le télécommunicateur à lui communiquer les renseignements. Lorsque l'ordonnance a été délivrée, la personne-ressource du télécommunicateur avait quitté pour la fin de semaine et la police a dû attendre trois jours avant d'obtenir les renseignements. Lorsque le télécommunicateur lui a communiqué les renseignements, la police les a utilisés pour obtenir un mandat supplémentaire autorisant la perquisition d'une résidence. Une jeune personne a été arrêtée et détenue en attendant une évaluation de sa santé psychologique.

<u>Exemples de l'utilité des renseignements de base sur les abonnés pour localiser ou identifier une personne</u>

8) En 2008, la police de Calgary faisait enquête sur des courriels menaçants envoyés à une femme par une personne dont l'identité était dissimulée. Les autorités ont fourni au télécommunicateur l'adresse IP et lui ont demandé l'adresse physique d'où les courriels avaient été envoyés. Les renseignements leur ont été communiqués, de sorte qu'en moins d'un jour, la police a pu identifier la personne envoyant les courriels menaçants et mener son enquête à bien. La personne a été accusée de harcèlement criminel et la victime a obtenu une ordonnance de non-communication à l'encontre de cette personne.

9) Un enfant a été enlevé en Colombie-Britannique en 2011. Une alerte Amber a été diffusée, et heureusement le suspect a libéré l'enfant. Cependant, le suspect n'avait pas été appréhendé et il n'avait pas été localisé. Poursuivant son enquête, la police a obtenu une adresse IP associée au suspect. Elle a communiqué directement avec le télécommunicateur, qui l'a informée de sa politique de ne pas communiquer de renseignements sur les abonnés à partir d'une adresse IP sans ordonnance de communication. La police a informé le télécommunicateur que le suspect avait déjà enlevé un enfant et que d'autres enfants couraient peut-être un risque. Le télécommunicateur a décidé de communiquer les renseignements, et le suspect a été localisé et appréhendé moins de 24 heures plus tard.

10) En 2008, le dirigeant d'un gouvernement municipal au Québec recevait des menaces de mort et des appels de harcèlement. Dans ce cas, le télécommunicateur a coopéré et communiqué des renseignements de base sur les abonnés à la police lorsqu'elle les lui a demandés. La police a pu localiser et arrêter le suspect. Lors de l'arrestation, la police a saisi des armes dans la maison du suspect.

11) Le Service de police de Toronto a traité au moins deux affaires où des citoyens l'avaient appelé pour l'informer qu'ils communiquaient par Internet avec des personnes menaçant de se suicider. Dans les deux cas, les victimes potentielles n'étaient pas localisées. La police a communiqué avec les hôtes des sites Web et a reçu les adresses IP associées aux menaces de suicide. Elle a ensuite communiqué avec les télécommunicateurs et obtenu sans ordonnance

judiciaire les renseignements de base sur les abonnés. La police a ainsi pu localiser les personnes en détresse avant qu'elles ne puissent passer aux actes.

Exemples de l'utilité des renseignements de base sur les abonnés au début d'une enquête

12) En 2009, la police est intervenue à la suite d'un homicide où la victime avait subi de multiples coups de couteau et avait été abandonnée dans la rue. Elle a déterminé que la victime avait eu une altercation après avoir fréquenté un pub local. Un ami de la victime a dit à la police qu'un des hommes soupçonnés d'être impliqués dans le meurtre avait téléphoné au numéro cellulaire de la victime avant le meurtre. La police a examiné le téléphone de la victime et trouvé le numéro de téléphone cellulaire de ce suspect. Elle a ensuite fourni ce numéro à un télécommunicateur et obtenu les renseignements de base de l'abonné associé à ce numéro. Elle a ainsi pu identifier le suspect et, par la suite, d'autres suspects. Comme elle avait besoin de renseignements en plus des renseignements de base sur les abonnés, elle a demandé une ordonnance de communication et obtenu des messages texte incriminants.

13) En 2009, une entreprise de Calgary comptant 15 000 employés a été victime d'une intrusion dans son serveur. Une grande quantité de données de l'entreprise a été volée, y compris des dossiers personnels et des renseignements sur la paie. Au cours de son enquête, la police a obtenu une adresse IP de l'entreprise, identifié le télécommunicateur pertinent et demandé à ce télécommunicateur le nom et l'adresse du client associé à l'adresse IP. Le télécommunicateur a refusé de communiquer les renseignements de base sur les abonnés à la police de façon volontaire. La police a donc obtenu un mandat de perquisition, et les renseignements lui ont été communiqués cinq jours plus tard. Les renseignements ont permis à la police d'obtenir un mandat de perquisition à l'égard d'une résidence au Manitoba. En exécutant le mandat, la police a saisi les ordinateurs d'un ancien employé de l'entreprise. Le délai s'est toutefois avéré préjudiciable à l'entreprise puisque les renseignements qui avaient été volés revêtaient un grand intérêt pour les concurrents de l'entreprise.

Exemples de la nécessité d'une capacité d'interception

14) En 2008, des membres d'un groupe du crime organisé en Colombie-Britannique commandaient à un agent de commettre des actes criminels tels qu'extorsion et trafic de drogue, par le biais de messages transmis par téléphone cellulaire. Le fournisseur de services n'avait pas le moyen d'intercepter ces messages et il a fallu six semaines à la GRC pour mettre au point une solution technique. L'incapacité de la police d'intercepter des messages texte à un moment critique de son enquête l'a empêchée d'obtenir des éléments de preuve vitaux.

15) La GRC avait installé chez un fournisseur de services de l'équipement à l'appui d'une enquête internationale sur le blanchiment d'argent et le trafic de drogue. Lorsqu'une autre enquête internationale sur le terrorisme a été lancée, la police a dû réaffecter l'équipement mis en place pour l'enquête sur le blanchiment d'argent afin d'intercepter les communications de la cible principale de l'enquête sur le terrorisme. Par conséquent, des éléments de preuve ont été perdus dans le cadre de l'enquête sur le blanchiment d'argent. Si les télécommunicateurs avaient été obligés de disposer d'une capacité d'interception, les deux interceptions auraient pu être effectuées et aucun élément de preuve n'aurait été perdu.

L'Association canadienne des chefs de police a obtenu de nombreux autres exemples de l'utilité des renseignements de base sur les abonnés à l'application de la loi. Ils seront abordés au moment des travaux en comité.

Thompson, Julie

From: Thompson, Julie
Sent: Thursday, October 25, 2012 11:22 AM
To: Hawrylak, Maciek
Subject: RE: Lawful interception in India
Attachments: MIG -Ready_Guide_2_Apr2008 FINAL.PDF

s.21(1)(b)

Thanks for the feedback. [redacted] You probably already have this document but the section about India's lawful interception legal framework was attached with the briefing.

Just to let you know, the briefing never reached Lynda and Bob as we did not obtain a formal request for this tasking...

Julie

Julie Thompson
Policy Analyst/Analyste en politiques
Investigative Technologies and Telecommunications Policy/Politiques sur les technologies d'enquête et les télécommunications
National Security Operations Directorate/Direction des Operations de Sécurité Nationale
Public Safety Canada/Sécurité Publique Canada
Tel: 613.998.7893
Email/Courriel : julie.thompson@ps-sp.gc.ca

From: Hawrylak, Maciek
Sent: October-25-12 11:07 AM
To: Thompson, Julie
Subject: RE: Lawful interception in India

Hi Julie,

Just a question here. Under your passage about India, you note that "Unlike Canada, India has a legal framework that governs lawful interception". I think this might be a bit misleading. Canada has a legal framework that governs lawful interception – it's Part VI of the Criminal Code. What Canada doesn't have (and India might or might not), is legislation requiring TSP's to have intercept-capable networks.

It is also unclear to me, from the rest of the paragraph, whether India just has lawful interception legislation (like us), or interception capability legislation (unlike us).

Just a couple of thoughts. Thanks!

Maciek

From: Thompson, Julie
Sent: October-25-12 10:24 AM
To: Hawrylak, Maciek; Scott, Marcie
Subject: Lawful interception in India

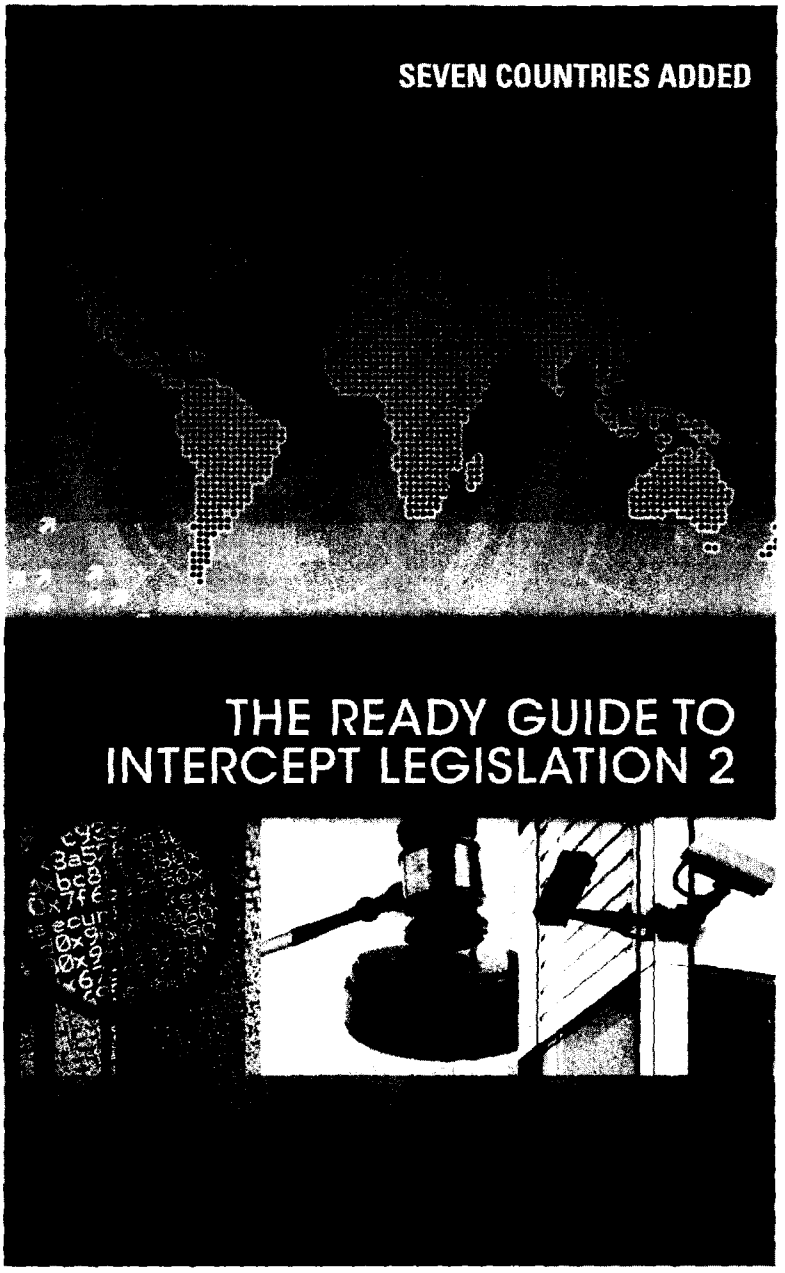
Good morning,

Marie has asked me to share a copy a briefing note (RDIMS# 707802) that we produced for the ADM's visit to India as you are working on comparing lawful intercepti . If you have any question, let me know.

Julie

doc not recorded for trip etc was deleted from RDIMS

Julie Thompson
Policy Analyst/Analyste en politiques
Investigative Technologies and Telecommunica chnologies d'enquête et les télécommunications
National Security Operations Directorate/Direct Nationale
Public Safety Canada/Sécurité Publique Canada
Tel: 613.998.7893
Email/Courriel : julie.thompson@ps-sp.gc.ca



ABOUT THIS GUIDE

Famed author, Henry Miller, once said, "The legal system is often a mystery, and we, its priests, preside over rituals baffling to everyday citizens." In this guide, SS8 has endeavored to identify and summarize this [oft baffling!] legislation, governing lawful intercept within a select number of countries around the world. Information detailing the legislation and policies within these 31 countries is garnered from various open sources and should not be considered conclusive. On the other hand, this guide is free! But should you wish to spend more, we leave the interpretation of these laws to the experts. For as the businessman Franklin P. Jones stated, "Anybody who thinks talk is cheap should get some legal advice."

ABOUT SS8 NETWORKS

Today's electronic surveillance requirements place rigorous yet different demands on carriers and law enforcement agencies. Carriers need to be able to quickly and efficiently identify a target in their network, isolate that target's traffic and get it to law enforcement in a standard, reliable, and legally compliant manner. In turn, law enforcement needs to perform detailed analysis of this information in order to build the story of the target's activities and interactions. Above all, governments need to feel confident that interception capabilities are ahead of the criminal mind. These diverse but intertwined needs are ideally met with an Xcipio-based solution from SS8 Networks.

SS8 Networks is the recognized independent leader in lawful intercept and a worldwide provider of regulatory compliant, electronic surveillance solutions. For nearly fifteen years we have been building networks, futures, cases [for the prosecution] and relationships. Our comprehensive product portfolio covers all three functions of the de facto lawful intercept (LI) architecture: access, mediation and collection. We have deployed proven lawful intercept solutions on all continents, in the networks of the largest wireline, wireless and cable carriers, while also creating non-traditional solutions that include satellite voice carriers, satellite ISPs and WIFI hotspots. Our installations can intercept over 500 million subscribers, and serve over 10,000 law enforcement agents.

SS8 Networks has grown a team with unequalled core competence, a heritage that is undeniable and a solution set that is unparalleled. As the safe choice for carriers, LEAs and governments the world over, SS8 will leave you confident that obligations for national security, criminal prosecution and traffic interception can be fulfilled.

SS8 Networks THE ARCHITECTS OF INTERCEPTS™

TABLE OF CONTENTS

AUSTRALIA

Law Name	Telecommunications (Interception and Access) Act 1979
Related Legislation	1. National Crime Authority Act, 1984 2. Telecommunications Legislation amendment bill, 1997 3. Telecommunications Interception Legislation Amendment Act, 2002 4. The stored communications amendment to the interception act, 2004 5. Telecommunications (interception) amendment bill, 2006
Parties Responsible for Enforcing or Certifying	1. Administrative Appeals Tribunal 2. Attorney General 3. Australian Federal Police 4. Australian Crime Commission 5. Australian Security Intelligence Organization

The first Australian act to legislate interception was the Telephonic Communications Act of 1960. More substantial provisions were made in the Telecommunications (Interception and Access) Act 1979,[1] while other statutes and amendments followed over time. These included the National Crime Authority Act 1984; the Telecommunications Legislation Amendment Bill 1997; the Telecommunications (Interception) Legislation Amendment Act 2000; the Telecommunications Interception Legislation Amendment Act 2002; the Stored Communications Amendment to the Interception Act 2004 and the Telecommunications (Interception) Amendment Bill 2006.

The Telephonic Communications (Interception) Act, 1960 prohibited the interception of communications except under two particular circumstances – threats to national security and drug trafficking. This law was repealed and replaced by the Telecommunications (Interception) Act 1979 (the Interception Act).

The primary objective of the Act of 1979 is to protect the privacy of Australian citizens using any Australian telecommunication channel. However, the exceptions mentioned in paragraph 7(2) (b) continue to authorize the process of legal interception of a communication channel under circumstances of serious offences or national security. Under this act, the law enforcement agencies, such as the Australian Federal Police (AFP) and the Australian Crime Commission (ACC), were for the first time legally allowed to intercept communications. A warrant was required from the law enforcement agencies or the Australian Security Intelligence Organization (ASIO) to authorize this interception.

The Australian Federal Police (AFP) is required to maintain a register of interception instances and submit it to parliament every three months. Section 49 of the Act limits the maximum duration of an issued warrant to 90 days. The Act of 1979 was derived from section 51 of the Australian Constitution Act which gives Parliament the authority to form laws for general peace and order. Amendments made to the bill in 2004 govern interception of stored data.[2]

The first amendment to the act of 1979 was instituted in 1997 and applied to telecom operators, ISPs and carriage service providers (CSPs). The act obligated operators to protect the confidentiality of all communications except when disclosure of relevant information was required and authorised by law.

In 2002, the Telecommunications Interception Legislation Amendment Act was passed. It sought to counter the shortcomings of the previous act and also grant more surveillance powers to the government. It brought into its purview offences involving acts of terrorism, child pornography, etc.[3] On December 8, 2004 the Senate passed the Surveillance Devices Bill, which regulated the use of listening and tracking devices by law enforcement agencies.[4] Prior to that, in November 2004, the Australian Senate passed the 'Stored Communications Amendment to the Inter-

ception Act'. The amendment sought to remove the protection of interception of emails, SMS, and voice mail messages that had not been delivered. By removing the protection, the senate allowed the authorities to intercept the above communications channels without a warrant. The Act however, did not include communication channels such as VoIP.[5] In November 2005, the US Department of Justice expressed the need for the Australian Senate to add coverage of VoIP interception in its legislation.[6] The law was further modified on June 13, 2006 by the Telecommunications (Interception) Amendment Bill 2006 that addressed the content or substance of stored communication (distinct from address of origin and termination) and it obligated law enforcement agencies to provide a 'stored communications warrant' before interception.[7]

The Interception Warrant for National Safety issues can only be issued by the Attorney General. Under special circumstances when the Attorney General (AT) is not in a position to issue the warrant, then it can be issued by the director general of security and approved by the AT. This is unlike law enforcement warrants that can be issued by an eligible judge or a member of the Administrative Appeals Tribunal (AAT).

Warrants issued for the interception of any communication medium, are provided only under the thorough scrutiny of the warrant issuing authorities and only after they have confirmed the extent of the offence and are convinced that all other methods of surveillance have been duly exhausted.

1 Source : http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/
2 Source : http://www.ag.gov.au/
3 Source: http://www.legco.gov.hk/yr04-05/english/sec/library/0405rp02e.pdf
4 Source : http://www.efa.org.au/Issues/Privacy/sd_bill2004.html
5 Source : http://parlinfoweb.aph.gov.au/piweb/Repository/Legis/Bills/Linked/27050402.pdf
6 Source: http://caia.swin.edu.au/talks/CAIA-TALK-060209A.pdf
7 Source: http://www.efa.org.au/Issues/Privacy/ta.html#laws

AUSTRIA

Law Name	Code of Criminal Procedure, 1975
Related Legislation	1. Strafrechtsänderungsgesetz, 2002 2. Überwachungsverordnung, 2001 3. Telecommunications Law 2003
Parties Responsible for Enforcing or Certifying	Court

The Code of Criminal Procedure[8] 1975, also known as Strafprozessordnung (StPO), is the law regulating lawful interception, wiretapping, electronic surveillances, and computer searches in Austria. Other statutes containing provisions for the interception of telecommunications include the amendment BGBl.I 134/2002 (also known as Strafrechtsänderungsgesetz 2002)[9], Überwachungsverordnung[10] (ÜVO), February 2001 and the Telecommunications Law[11] 2003, also known as Telekommunikationsgesetz (TKG 2003). Under UVO, compliance deadlines were set for telecommunication equipment operators (1 June 2001 in accordance with Sections 3 and 4) and network operators (1 January 2005 for compliance with technical handover interface requirements).

Wiretapping provisions are also included in the Code of Criminal Procedure under sections 149a to 149p. Like many statutes that seek to protect privacy, Section 149c (7) of the Code of Criminal Procedure states that the intercepted information needs to be erased in instances where the information has no appropriate use. This Act was further amended on October 1, 2002. The amendment, BGBl. I 134/2002 added new cyber crimes to the list of offences susceptible to lawful intercept and amended some of the prevailing sanctions regarding cyber crime.

In Austria, wiretapping can only be approved, by a judge, for the investigation of criminal cases where the crime is punishable by more than one year in prison. Electronic surveillance, along with

computer access, is authorized for crimes that are punishable by more than 10 years in prison. The stipulations for electronic surveillance and computer access were enforced between 1 October 1997, and 1 July 1998.[12]

In August 2003, the Telecommunications Law 2003 was enacted and obligated telecom operators to provide the necessary surveillance equipment to support lawful interception. According to Section 94 (1) of TKG 2003, telecom operators are required to procure all equipment necessary for the interception of telecom services as stated in the provisions of the Code of Criminal Procedure. Also, according to Section (2) of TKG 2003, the provider has to participate in the interception of the telecom service only to the extent required by law. These obligations apply to all commercial telecom services that broadcast signals over communication networks.

Another ordinance issued in September 2004, by the Federal Minister of Justice, specified that the telecom operators could be compensated on a per-case basis for costs incurred in providing surveillance.[13] The reimbursement included the costs for staff and installation, maintenance, and monitoring of the surveillance equipment.

A draft ordinance, Überwachungsverordnung (ÜVO) was issued in February 2001 by the Federal Minister of Transport, Innovation and Technology, which obligated all telecom operators to install technical equipment for facilitating the surveillance and interception of telecom traffic in compliance with the Code of Criminal Procedure.

According to Section 4 (1) ÜVO, the transmission of the intercepted telecommunication should be performed using standardized transmission paths and protocols. It further specified that carriers must comply with ETSI standard ('201 671 V 1.1.1'[14]), that specifies the handover interface of lawfully intercepted telecom-

munications traffic. Section 4 (2) specifies that for transmission purposes, fixed lines or ISDN dial-up (or similar) connections should be used. In case of dial up connections, the interface should be capable of automatically connecting to the recording device. Also when using a dial-up connection, a connection will be established at the start of each transmission of intercepted telecommunication and released after its completion. According to Section 4 (5), the interception process needs to be kept secret so that neither the suspect nor anyone else knows about it. Moreover, it specifies that the operation of the intercepted subscriber line should not be altered by the surveillance process.

The telecom provider must be capable of providing any intercepted information that is required by the authorities. This includes the address of the subscriber line under surveillance, along with the numbers of all inbound and outbound call attempts, whether they are successful or not. The service provider also needs to track the start time, end time, and the total duration of the call. In the case of mobile phone users, a record of all dialled numbers needs to be maintained. Subject to the court's permission, the authorities can request both the exchange data and the content data from the service provider. The service provider is not only required to assist the authorities in interception but is also obliged to deliver the intercepted information to law enforcement agencies.

8 Source: http://www.internet4jurists.at/gesetze/bg_stpo01.htm
9 Source: http://www.csirt-handbook.org.uk
10 Source: http://www.vibe.at/misc/uevo.en.html
11 Source: http://64.233.179.104/translate_c
12 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005Arg-Chile.pdf
13 Source: http://ris1.bka.gv.at/authentic/findbgbl.aspx?name=entwurf&format=html&docid=COO_2026_100_2_117197
14 Source: http://www.opentap.org/documents/ES201-671.pdf

ARGENTINA

Law Name	The National Intelligence Law No. 25.520, 2001
Related Legislation	1. Information and Intelligence Organic Law 2. Information and Intelligence Control Law 3. Internal Security Law 4. National Defence law 5. Decree No. 950, 2002
Parties Responsible for Enforcing or Certifying	National Directorate for Criminal Intelligence under the jurisdiction of the Minister of Justice, Security and Human Rights

In 1990, Argentina introduced the Information and Intelligence Organic Law; it included a provision for judicial control of interception. Later, in 1993, the Information and Intelligence Control Law was introduced; the bill was a modified version of the Information and Intelligence Organic Law and defined provisions such as technical operations of approved intercepts and penalties for violating the law relating to legal interception. However, in 1995, the United Nations Human Rights Committee expressed its concern over the breadth of the law and this led to the introduction of the National Intelligence Law No. 25.520, which was enacted in November 2001.[15]

Title VI of the National Intelligence Law — Interception and Seizing of Communications — defines provisions for lawful interception and requires operators to have technical capabilities that intercept and forward intercepted communications to the investigating authorities. The law was enhanced in 2002 when a decree was introduced that required telecom operators and ISPs to decrypt their customers' encrypted communications, if the operator was providing the encryption capabilities as part of their service to the customer. It also mandated that operators could not disclose the technical and administrative methods used to comply with their lawful intercept obligations. Such a decree received protests from ISPs and the public; in April 2005, the President

suspended the decree. Currently, the decree is under a process of evaluation for re-introduction.

Under Law 23.984, any investigating authority, requesting an electronic surveillance, needs prior approval from the judiciary;[16] the Secretary of Intelligence is required to file a written request for judicial approval with the Directorate for Judicial Observations or an equivalent judicial authority. Legal requirements *for ISPs to build surveillance and wiretapping capabilities are* becoming more common with the National Intelligence Law detailing how telecom companies should collaborate with the intelligence agencies to wiretap communications traversing their networks. Further, orders to conduct wiretapping surveillance are only valid for up to 60 days, although the grant can be renewed for another 60 day period. Also, if the government decides not to initiate criminal proceedings against the accused, all evidence collected through the surveillance must be destroyed by the investigating authorities.

There is an exception clause in the bill (under Section 10) which states that the interception warrant is not required in cases of emergency and in circumstances where threats of terrorism or organized crime might pose a danger to property or the lives of individuals. In such cases, communications can be taped without prior judicial order. Intelligence agents are allowed to secretly search, observe, examine, take photographs, record, copy documents, download, or electronically transmit computer media without the need for judicial authorization.[17]

15 Source: http://infoleg.mecon.gov.ar, http://www.dcaf.ch/legal_wg/ev_oslo_030919_estevez.pdf
16 Source: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-103798
17 Source: http://pi.gn.apc.org/article.shtml?cmd%5B347%5D=x-347-359596&als%5Btheme%5D=Anti%20Terrorism

BELGIUM

Law Name	1. 'wet van 30 juni 1994-ter bescherming van de persoonlijke levenssfeer tegen het afluistereren, kennisnemen en openen van privécommunicatie en telecommunicatie' 2. Loi du 10 juin 1998
Related Legislation	13 Art 259 Code Penal, 30 June 1994
Parties Responsible for Enforcing or Certifying	1. Judicial Police, Investigation Judge, 2. Attorney General, 3. BIPT

The law 'wet van 30 juni 1994-ter bescherming van de persoonlijke levenssfeer tegen het afluistereren, kennisnemen en openen van privécommunicatie en telecommunicatie' regulates lawful interception in Belgium. The provisions include the interception of private conversations and private telecommunications. Prior to the enactment of this law, there was no specific law dealing with lawful interception in Belgium[18].

Surveillance activity conducted under this law can only be executed after a warrant is granted by the investigation judge. Such warrants are granted only in cases where the target is involved in serious crimes such as terrorism. The nominated duration for such surveillance is one month; however, in some circumstances it can be extended by up to six months, after which a new application [for performing surveillance] must be lodged. Unwarranted surveillance activities, such as monitoring, recording, and listening to private communications and private telecommunications (except for the cases described/authorized by the law), are punishable under 13 Art 259 of the Penal Code, 30 June 1994. In cases where the surveillance requires co-operation from telecom operators, the investigation judge must issue orders both to the judicial police and the telecom operator; telecom operators are only required to provide technical assistance during the surveillance. The law also requires that all communications monitored

during the surveillance be recorded and that such recordings be submitted to the investigation judge.

The "wet van..." law was amended in 1997 to remove restrictions on encrypted messages. According to the amendment, the investigation judge could now request experts or network managers to help decrypt intercepted telecom messages; refusal to co-operate for such requests could in turn lead to criminal prosecution.[19] An additional amendment in 1998 mandated greater assistance from telecom operators in performing surveillance and provided more power to the investigation judge and the Attorney General.

According to the law, telecom operators and service providers were also required to record and store calling data and subscribers' identification data for a minimum period of 12 months. In 2003, a new royal decree was enacted to enforce the 'Loi du 10 juin 1998' and provided more details on the practical and technical measures that telecom operators and service providers must comply with to cooperate with law enforcement authorities.

After the adoption of the Interception Law in Belgium in 1994, the number of orders issued for wiretapping increased from 114 in 1996 to 1,000 in 2002, and 1,336 in 2003 to 2,562 in 2004. This increase can be attributed to the increased availability of technical assistance with the creation of the Central Technical Interception Facility (CTIF). In 2005, the number of intercepts per 100,000 inhabitants was 24.4.[20]

18 Source: http://www.cryptome.org/za-esnoop.htm
19 Source: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83525
20 Source: http://www.edri.org/edrigram/number3.12/wiretap

BRAZIL

Law Name	Law 9.296, July 24, 1996
Related Legislation	1. The Telecommunications Act, 1997 2. Code of Criminal
Parties Responsible for Enforcing or Certifying	1. Judge-in-charge 2. Federal police

Law 9.296[21] was introduced in Brazil in 1996. Is purpose was to regulate the constitutional right that protects data and telecommunications privacy. Previously, such surveillance was an ad hoc process without any legal binding.

The new law required the police authority or prosecuting attorney to obtain prior permission from the judge-in-charge for any wiretapping of a suspect. Permission for wiretapping would be granted to the investigating party within 24 hours of filing of the request. Permission to perform a surveillance would only be granted if the suspect was involved in serious crimes, such as corruption, contraband smuggling, murder, kidnapping, or drug smuggling, and there were limited other means to collect evidence against the suspect. Hence, wiretapping is currently only allowed in criminal investigation cases.[22] The law also empowered police authorities to request technical assistance in performing electronic interception

In cases where the interception of telephonic or other electronic communication is undertaken without proper judicial authorization, the individuals involved in such exercise are liable to be prosecuted under Law No 9.296/96.[23]

A wiretap can only be carried out for 15 days, after which the surveillance warrant must be renewed for another 15 days by the judge.[24] After the surveillance is complete, any intercepted communication must be documented for legal usage and complete secrecy must be maintained. In cases where the investigating team is involved in insertion of false data, the members of the

investigating team are liable to be prosecuted, with a prison sentence of up to 12 years, and detention of up to two.

Despite the introduction of law for legal interception, illegal wiretapping by police and intelligence agencies is still common. Examples include the illegal interception of communications involving Itamar Franco, former Vice President of Brazil and illegal communication wiretaps on ministers involved in the Telegate scandal. In addition, a number of inherent weaknesses exist, including resistance on the part of the judges to grant authorization for interception, lack of stringent laws for telecom operators to support such surveillance activities, and insufficient time granted for carrying out such surveillance, which hamper the effectiveness of the law in the country.

21 Source: http://translate.google.com/
22 Source: http://www.oecd.org/dataoecd/12/45/35445196.pdf
23 Source: http://www.informaworld.com/smpp/content~content=a749183160~db=all
24 Source: http://courses.cs.vt.edu/~cs3604/lib/Privacy/International/Group1/GROUP1.HTM

CANADA

Law Name	Criminal Code, 1974
Related Legislation	1. Canadian Security Intelligence Service Act, 1984 2. Competition Act 3. Modernization of Investigative Techniques Act, 2005
Parties Responsible for Enforcing or Certifying	1. Judge 2. Canadian Security Intelligence Service 3. Minister of Public Safety and Emergency Preparedness 4. Commissioner of Competition

At present, the Criminal Code[25] is the primary legal framework that governs the interception of telecommunications in Canada. Other statutes that have a provision for lawful intercept include the 1984 Canadian Security Intelligence Service Act (CSIS)[26] and the Competition Act[27]. Another law that has died twice on the house floor is the 2005 Modernization of Investigative Techniques Act (MITA)[28] and the current government doesn't have plans currently to resurrect it.

The provisions for intercepting communications under the Criminal Code were first adopted on July 1, 1974[29]. Under this legislation, the interception of telecommunications is permitted for the investigation of serious crimes, such as hijacking, sabotage, murder, etc. The specific provisions governing the interception of telecommunications are defined under Part VI of the Criminal Code (Invasion of Privacy) in Sections 183–196. Procedurally, according to Section 185.1, the application for obtaining a warrant for authorization has to be made in writing to a superior court judge with criminal jurisdiction. The issued authorization is then valid for a maximum period of sixty days. In exigent cases, the judge can issue an oral authorization, which remains valid for a period of thirty-six hours. Section 184.1(3) further requires the destruction of all intercepted information if no evidence of crime is found within it.

In a majority of cases, the criminal code does not allow for intercepted information to be admissible as evidence in legal proceedings, however there are certain exceptions. One of these situations is defined under Section 189(5) of the Criminal Code; it allows for the admissibility of intercepted communication as evidence in criminal proceedings, only if the prosecution has given practical notice to the accused, along with a transcript of the intercepted communications that contains the particulars (time, date and place) of the communication. Another situation falls under Section 184.1(2), according to this section intercepted information is admissible as evidence only in those court proceedings where suspected or actual bodily harm is alleged,

In 1984, the Canadian Security Intelligence Service Act was passed and it established the Canadian Security Intelligence Service (CSIS). Section 21 of the Act empowered CSIS to intercept telecommunications for safeguarding the national interests of Canada and defined procedures to obtain authorization for lawfully intercepting communications. The duties of the Service included collection, analysis, and retention of intelligence information. An authorizing warrant can be obtained by the CSIS Director or any employee of the Service by submitting a written application to a judge, after gaining prior approval from the Minister of Public Safety and Emergency Preparedness (PSEP). The warrant is issued for a maximum period of one year. According to Section 26 of the CSIS Act, provisions of Part VI of the Criminal Code do not apply to interceptions authorized under Section 21 of the CSIS Act.

Canadian statutes obligate the telecommunications service providers (TSPs) to cooperate with the government and the LEAs in conducting surveillance and intercepting any communication that arouse suspicion. The Modernization of Investigative Techniques Act (MITA), that has failed to pass into law so far, was designed to ensure that lawful intercepts can be successfully carried out even with the advent of new technologies (wireless, internet

based, VoIP, satellite etc. It would authorize the LEAs and CSIS to collect subscriber contact information from the TSPs that includes names, addresses, telephone numbers, Internet Protocol addresses, etc. It also includes a clause that obligates TSPs to decrypt or decode transmissions that they have control over before sending them to the LEAs.

There are certain provisions for interception of communications that prohibit malpractices within trade and commerce. The Competition Act, for example, enables interception of communications for the purposes of preventing deceptive marketing practices, telemarketing, price fixing, and bid-rigging. The Commissioner of Competition (as appointed by the Governor in Council) is responsible for administering and enforcing the Act.

The total number of video and audio authorizations and renewals that were applied for and granted under the Criminal Code alone during 1995–99 ranged between 149 and 281 per year. And for the years 2001, 2002, 2003, 2004 and 2005, there were 152, 180, 110, 141, and 106 applications for audio and video authorizations and renewals respectively.[30]

25 Source: http://laws.justice.gc.ca/en/showtdm/cs/C-46
26 Source: http://laws.justice.gc.ca/en/ShowTdm/cs/C-23///en
27 Source: http://laws.justice.gc.ca/en/showtdm/cs/C-34
28 Source: http://www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=2334024&file=4
29 Source: http://www.canada.justice.gc.ca/en/cons/la_al/g.html#26
30 Source: http://ww2.ps-sp.gc.ca/Publications/Policing/Esurveillance, http://www.publicsafety.gc.ca/abt/dpr/le/

ESTONIA

Law Name	Surveillance Act, 1994
Related Legislation	1. Constitution of the Republic of Estonia 2. Telecommunications Act 3. Code of Criminal Procedure 4. Electronic Communications Act
Parties Responsible for Enforcing or Certifying	1. Head of a Surveillance Agency 2. Tallinn Administrative Court 3. Tallinn City Court 4. National Security Police Commissioner 5. National Police Commissioner 6. Prosecutor

The Surveillance Act[31], 1994, enforced on March 18, 1994, is the primary legislation that regulates covert surveillance and interception of communications in Estonia. Other legislation that contains provisions for lawful intercept include the Telecommunications Act, 2000[32], the Code of Criminal Procedure[33] enacted on February 12, 2003, and the Electronic Communications Act[34], 2004. Provisions for lawfully intercepting communications are also listed in the Constitution of the Republic of Estonia[35].

The processes and procedures to conduct surveillance are outlined in the 1994 Surveillance Act. According to the act, the interception of communications is permitted for the purposes of detecting and preventing criminal activities. Subsection 10 (1) of the 1994 Act states that authorization, from either the head of a surveillance agency[36] or an official authorized by the head of a surveillance agency, is required before initiating the surveillance. Provisions for "special[37] and exceptional[38] surveillance activities" are defined under Section 12 of the Act and are permitted only when it is impossible to gather relevant intelligence information using conventional surveillance techniques (Subsection 12 (6)). Wiretapping and the recording of communications is permitted as an "exceptional surveillance" activity under Subsection 12 (2) and can only be conducted by the Security Police Board or

Police Board. Procedures for obtaining authorization to perform "exceptional surveillance" are listed under Section 13. According to Subsection 13 (1), a judge of the Tallinn Administrative Court can authorize "exceptional surveillance" methods upon receiving a written application from the National Security Police Commissioner, the National Police Commissioner, or any official required to conduct "exceptional surveillance" activity. These authorizations are valid for two months and can be extended for another two month term.

Provisions to conduct wiretapping and covert surveillance for investigation in criminal cases are defined in the Code of Criminal Procedure, enforced on July 1, 2004. These provisions are defined under Sections 110–122 of Division 8 ("Collection of Evidence by Surveillance Activities") of this legislation. The information collected through surveillance is used for the purpose of gathering evidence and is defined under Section 110—"Admissibility of Surveillance Activities in Collection of Evidence". The provisions and procedures for obtaining permission for surveillance activities are listed in Section 114 of the Act. According to it, an authorization is granted by a judge of a Tallinn City Court upon receiving an application from the Prosecutor. These authorizations are valid for two months and can be further extended by another two months. The use of covert surveillance of telegraphic items and wiretapping in criminal proceedings is permitted under Sections 116 and 118, respectively.

The Telecommunications Act of 2000 obligated the telecommunication service providers (TSPs) to provide information related to any subscriber upon receiving an oral or written request from an LEA. This Act was replaced by the Electronic Communications Act in order to comply with EU legislation. Obligations of TSPs to assist LEAs in intercepting communications are now defined in the Electronic Communications Act, enforced on January 1, 2005.

Obligations of TSPs to provide information and access to the communications network are defined under Sections 112 and 113 of the Electronic Communications Act. According to Section 112, LEAs can request TSPs to provide, within 10 working days, information such as messages sent and received, as well as the location of the sender and the receiver. In the case of urgent requests, TSPs are obliged to provide the information within 24 hours. Section 113 stipulates that the TSPS must provide LEAs with access to their networks for the purpose of interception but the costs incurred by TSPs to assist LEAs in intercepting communications is compensated by the government under Section 114 of the Act. The government compensation includes the cost of hardware and software, and the maintenance of equipment required for intercepting communications.

31 Source: http://www.era.int/domains/corpus-juris/public_pdf/estonia_surveillance_act.pdf
32 Source: http://sa.riik.ee/atp/failid/Telecommunications_Act.rtf
33 Source: http://www.legislationline.org/upload/legislations/07/a7/1f0a92298f6ba75bd07e101cdb93.htm
34 Source: http://www.riso.ee/en/node/45
35 Source: http://www.president.ee/en/estonia/constitution.php
36 Surveillance agencies include Security Police Board, Police Board, Border Guard Administration, Headquarters of the Defense Forces and Prisons Department of the Ministry of Justice and prisons (Subsection 6 (1)).
37 Special surveillance activities include covert collection of information and comparative samples, covert examination of documents and objects, covert surveillance, and covert identification (Subsection 12 (1)).
38 Exceptional surveillance activities include covert entry into premises, data banks, workplaces.; installation of technical appliances; covert examination of postal items; wire tapping; recording of messages and other information transmitted through technical communication channels, such as telegraph, telephone; and staging of criminal offences (Subsection 12 (2)).

FINLAND

Law Name	Coercive Means Act (Chapter 5a), 1987
Related Legislation	1. Act on the Protection of Privacy in Electronic Communications, 2004 2. Act 1995/402 3. Police Act, 2001
Parties Responsible for Enforcing or Certifying	1. Court 2. The Finnish Communications Regulatory Authority

Lawful interception in Finland is governed by the Coercive Means Act (Chapter 5a), as amended by the Act 1995/402. This Act includes provisions for the metering of telecommunications, bugging of telecommunications, and technical surveillance.[39] Telecommunication interception includes the interception of fixed-line telephones, mobile phones, and e-mails.

Authorization for performing interception is obtained through a court of law. The application for authorization has to be made in writing by the police or by an official who has the authority to arrest.[40] The wiretapping is only authorized if the intercepted information is considered to be of utmost importance to the case proceedings. Wiretapping is permitted in the investigation of serious crimes, such as skyjacking, narcotics offences, treason, etc. While interception warrants are valid for no more than one month, depending upon the severity of the situation, the police can file a new application for extension.

Metering of telecommunications (i.e acquiring intercept related information/call signalling) is authorized in investigations of computer crimes, drug-related crimes, or cases in which prosecution can lead to sentencing of at least four months in prison. However, telecommunications 'bugging' (interception of actual call content) is only granted for suspects accused of drug peddling or for any other crime in which the punishment is at least four years imprisonment.

Section 3 of the Police Act, 2001[41] authorizes the police to use technical surveillance and metering of telecommunications for reconnaissance purposes. Also, the Act on the Protection of Privacy in Electronic Communications,[42] which was enforced on September 1, 2004, expanded the scope for police access to telecommunication information in the investigation of criminal cases. The Act of 2004 replaced the Protection of Privacy and Data Security Act of 2000. It also expanded the definitions of telecommunications to include e-mails and all Internet-based communications. In all cases, the police are authorized to acquire a dynamic IP address and the international mobile equipment identity (IMEI) numbers of mobile phones. The Finnish Communications Regulatory Authority (FICORA) enforces these acts and ensures compliance.[43]

The number of intercepted cases in Finland is far fewer than in other European countries.

39 Source: http://www-rohan.sdsu.edu/faculty/rwinslow/europe/finland.html
40 Source: http://www.coe.int/t/dg1/Greco/evaluations/round2/GrecoEval2(2003)3_Finland_EN.pdf
41 Source: http://www.finlex.fi/en/laki/kaannokset/1995/en19950493.pdf
42 Source: http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf
43 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005china-georgia.pdf

FRANCE

Law Name	1. Code of Criminal Proceedings 2. Telecommunications Correspondence (Secrecy) Act, 1991
Related Legislation	1. Fiscal Procedure Code 2. Monetary and Financial Code 3. Data Protection Act 4. Posts and Telecommunications Code 5. Freedom of Communication Act 6. Decree No. 93-119 7. Decree No. 2002-997 8. Law for Interior Safety 9. Everyday Security Act
Parties Responsible for Enforcing or Certifying	1. Court 2. Ministry of Interior

There are many French laws regulating the lawful interception of telecommunications. The predominant legislation is the Telecommunications Correspondence (Secrecy) Act[44] (Loi sur le secret des correspondances, Law No. 91-646), July 10, 1991, otherwise referred to as the "1991 Act." Other statutes have also made provisions for lawfully intercepting communications: the Code of Criminal Procedure;[45] the Fiscal Procedure Code; the Monetary and Financial Code; the Data Protection Act[46] (Loi informatique et libertés, Law No. 78-17), January 6, 1978; the Posts and Telecommunications Code; the Freedom of Communication Act'[47] (Loi relative à la liberté de communication, Law No. 86-1067), September 30, 1986, as amended by the Law of August 1, 2000, the Decree No. 93-119, January 28, 1993; the Decree No. 2002-997[48], July 16, 2002; the Law for Interior Safety (Loi de Sécurité Intérieure, Law No. 2003-239) March 18, 2003; and the Everyday Security Act[49] (Loi sur la Sécurité Quotidienne or LSQ, Law No.2001-1062), November 15, 2001.[50]

Article 1 of the 1991 Act authorises the lawful interception of telecommunications. Telecommunication service providers are obligated to intercept communications when authorized under Articles 100 to 100–7 of the Code of Criminal Procedure, by an investigating judge, the Courts of Assize or by the French Supreme Court of Appeal (Cour de Cassation). The service providers are also required to intercept telecommunications in cases where authorization is granted by the Prime Minister. These interceptions are permitted for the prevention of serious offences, such as terrorism, espionage, or threat to national security. According to Article 11–1 of the 1991 Act, the telecommunication service provider is obligated to provide a decrypted version of encrypted information or alternatively to give the decryption keys to the authorities.

A warrant for interception is issued in writing and must contain the number of the intercepted subscriber and the duration of interception. Warrants are valid for a maximum period of four months but can be renewed under Article 6 of the 1991 Act. Article 9 of the 1991 Act mandates that law enforcement authorities destroy intercepted information, under the supervision of the Prime Minister, within 10 days of interception.

According to Article L.35-5 of the Postal and Telecommunications Code, service providers must provide access to all information required by the authorities. This information may include the most updated list of subscribers and users, their addresses and any numbers dialed.

Article D.98-1 of the Postal and Telecommunications Code compels service providers to work with LEAs in conducting electronic surveillance; operators are supposed to install and make available the technical equipment required for interception. Article D.99 states that any independent network operator shall

also comply with the LEAs in situations related to public safety or defence. Data can be retained by telecommunication service operators for a maximum of one year under the provision of Article L32-3-1 of the Postal and Telecommunications Code.

The costs for deploying intercept technology, and the subsequent maintenance thereof, are covered by the French government under Article 35-6 of the Postal and Telecommunications Code. Operating costs for performing interception and the cost of connections for transmission of intercepted information are also reimbursed by the government.

Other statutes with wiretapping provisions include 1) the Everyday Security Act (Article 22), which provides for the use of new technologies in the field of communication and information to prevent serious crimes, such as terrorism, narcotics, etc, 2) Decree No. 93-119, issued to appoint officials to supervise installations of the equipment necessary for providing interception in accordance with the 1991 Act, 3) Decree No. 2002-997, which covered telecommunication service providers carrying encrypted traffic, 4) The Law for Interior Safety, which prescribed the powers given to state and local authorities for the protection of people and goods, 5) The Data Protection Act, which covers the access to data and files, and 6) The Monetary and Financial Code, which grants powers to investigators to summon telecom operators to provide them with certain information.

For national oversight, the Commission nationale de contrôle des interceptions de sécurité (CNCIS) was created to lay down rules and regulations regarding interception of communication. CNCIS also has the responsibility for reviewing the number of wiretapping cases every year. The number of authorized interceptions of telecommunications from 1995 to 1999 was between

4,500 and 4,700.[51] There were 5,651 authorized interceptions in 2004. Of these, 3,733 were initial interceptions and 1,918 were renewals.[52] During 2005 and 2006, there were 5,774 (4,067 initial interceptions and 1,707 renewals) and 5,985 (4,176 initial interceptions and 1,809 renewals) official interceptions, respectively.[53]

44 Source: http://www.legifrance.gouv.fr/texteconsolide/PCEAR.htm
45 Source: http://195.83.177.9/upl/pdf/code_34.pdf
46 Source: http://195.83.177.9/code/liste.phtml?lang=uk&c=25&r=1061, http://www.legifrance.gouv.fr/texteconsolide
47 Source: http://www.legifrance.gouv.fr/html/codes_traduits, http://www.legifrance.gouv.fr/texteconsolide
48 Source: http://www.legifrance.gouv.fr/texteconsolide, http://www.legifrance.gouv.fr/texteconsolide
49 Source: http://www.legifrance.gouv.fr/texteconsolide, http://www.legifrance.gouv.fr/texteconsolide
50 Source: http://www.minez.nl
51 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005china-georgia.pdf
52 Source: http://www.ladocumentationfrancaise.fr/informations/presse/2005/interceptions-securite.shtml
53 Source: http://lesrapports.ladocumentationfrancaise.fr/BRP/074000237/0000.pdf

GERMANY

Law Name	1. Telecommunications Act, 2004 2. Telecommunications Interception Ordinance, 2002 3. The Act on the Restriction of the Privacy of Correspondence, Posts, and Telecommunications, 2001 4. Telecommunications Act, 1996 5. Criminal Procedure Code, 1987
Related Legislation	1. Foreign Trade and Payments Act, 1961 2. Customs Investigation Service Act
Parties Responsible for Enforcing or Certifying	1. Judge 2. Ministry of Interior

In Germany, lawful interception of communications through wiretapping and recording of IP-based network communication is approved by a number of statutes. The main laws governing the interception of telecommunications are the Criminal Procedure Code[54] (Strafprozeßordnung, StPO), April 7, 1987; the Telecommunications Act[55] (TKG), July 25, 1996; the Act on the Restriction of the Privacy of Correspondence, Posts, and Telecommunications (G-10), June 26, 2001; the Telecommunications Monitoring Regulation[56] (TKÜV), January 22, 2002 and the Telecommunications Act[57] (TKG), June 22, 2004. Other laws having provisions for wiretapping are the Foreign Trade and Payments Act (AWG), April 20, 1961, and the Customs Investigation Service Act (ZFdG).[58]

Interception can be carried out in criminal cases, such as homicide, narcotics, etc., or in cases of threat to the national security of Germany. Under Section 100a of the Criminal Procedure Code, such interceptions must be authorized by a judge. This authorization is given in writing and can remain enforced for a period of three to six months, according to Section 100b (2) of the Criminal Procedure Code. The German Minister of Interior can also order the interception of telecommunications. In cases of extreme urgency, the public prosecutor may authorize the interception.

The G-10 Act authorizes federal and state law enforcement agencies to intercept and record telecommunications and to open and scrutinize postal packets. The AWG authorizes the Customs Criminological Office to intercept and record telecommunications. Further details are included in Section 100(a) of the Criminal Procedure Code.

According to the definitions of 'telecommunications' and 'telecommunications systems' given in Section 3(16) and Section 3(17) of the TKG 1996, telecommunications covers all aspects of IP communications including VoIP, Web hosting, e-mail, and Internet services.

The German interception laws also impose obligations on telecom operators. Section 88 of the TKG 1996 states that the telecommunication service operator needs to configure and keep available technical facilities for implementing interception of According to Section 88 (2) of the TKG 1996, telecom operator systems are only permitted to operate when these interception facilities are approved by the Federal Network Agency, formally known as the Regulatory Authority for Telecommunication and Mail (Regulierungsbehörde für Telekommunikation und Post; RegTP). Section 2 of the G-10 law and Section 88 (4) of the TKG 1996 then clearly states that operators will use these capabilities to intercept call signaling and content. Operators are also compelled to hand over any e-mails transmitted over their networks, and to provide ready network access for transferring the intercepted information.

On June 22, 2004, the German Parliament adopted the Telecommunications Act complying with the European Parliament's decision to modify the existing telecommunications law in May 2002. Part 7 of this TKG 2004 includes all the provisions for privacy of telecommunications, data protection, and public safety. This Act, under Section 110, also requires telecom operators to deploy the

technical facilities necessary for implementing interception at their own expense.[59]

The TKÜV regulates the technical and organizational requirements for interception of telecommunications. This ordinance was amended in August 2002. Section 21 of the TKÜV provides for potential relaxation toward telecommunication operators with less than 10,000 subscribers; in section 3 (2)(5), TKÜV states that the obligations for service providers with less than 1,000 subscribers is limited to assisting authorities with intercepting and recording calls. All telecommunication companies need to align themselves to the stipulated technical standards in compliance with the legal obligations under TKÜV. These standards have been specified in the Technical Directive of TR TKÜ 3.1,[60] issued by the RegTP in May 2002. This directive was a joint effort of the service providers, law enforcement agencies, telecommunications equipment manufacturers, and regulatory authorities. January 1, 2005 was the stipulated deadline given by the TKÜV for providers to either procure new equipment or modify the existing equipment for interception with respect to the ordinance's directive.

There has been a quantum leap of nearly 500 percent in the number of wiretapping cases in Germany within a decade. In 1994, there were 4,674 cases of monitoring. By comparison, there were 29,017 cases of lawful interception in 2004.[61]

54 Source: http://www.iuscomp.org/gla/statutes/StPO.htm#100
55 Source: http://www.iuscomp.org/gla/statutes/TKG.htm
56 Source: http://217.160.60.235/BGBL/bgbl1f/bgbl102005s458.pdf
57 Source: http://www.bfdi.bund.de/cln_030/nn_946430/EN
58 Source: http://www.minez.nl/, http://cyber.law.harvard.edu/globaleconomy, http://www.datenschutz-berlin.de
59 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005china-georgia.pdf
60 Source: http://www.eco.de/servlet/PB/show/1223643/20030515-TR-TKUE-EN.pdf
61 Source: http://www.heise.de/newsticker/meldung/58104

HONG KONG

Law Name	Interception of Communications and Surveillance Ordinance (Cap 589), 2006
Related Legislation	1. Section 33 of Telecommunications Ordinance (Cap 106), 1963 2. Interception of Communications Ordinance (Cap 532), June 1997
Parties Responsible for Enforcing or Certifying	1. Chief Executive 2. Chief Justice 3. Panel Judges 4. Authorizing Officer 5. Commissioner on Interception of Communications and Surveillance

The Interception of Communications and Surveillance Ordinance (Cap 589), 2006[62] is the main legislation that governs the lawful interception of communication in Hong Kong. In June 1997, the Interception of Communications Ordinance (Cap 532) was enacted; the date of its commencement, however, was never promulgated.[63] Up until August 2006, the Telecommunications Ordinance (Cap 106)[64] regulated the interception of telecommunications in Hong Kong.

A panel of judges was created under the 2006 Interception of Communications and Surveillance Ordinance to authorize and supervise the use of interception and surveillance for lawful enforcement purposes. As per Division 1, Part 3 of the 2006 Ordinance, the Chief Executive, in consultation with the Chief Justice, appoints three to six panel judges for a three-year term. A panel judge is empowered to either grant or deny authorization for communication interception.

In Division 2, Part 3 of the 2006 Ordinance the methods for obtaining authorization for lawfully intercepting communications are defined. These methods detail the procedure for obtaining authorization from a panel judge for either a lawful intercept or a

Type I (covert) surveillance. The application for authorization has to be submitted in writing by an officer of an authorized department[65] to the panel judge. The authorization for interception remains valid for a maximum duration of three months from the date of its approval.

Law enforcement agencies (LEAs) are permitted to apply for Type 2 surveillance authorization under the 2006 Ordinance. Type 2 surveillances are defined in the Interception of Communications and Surveillance Ordinance, as any covert surveillance using either a listening device or an optical surveillance device. The procedure to obtain executive authorization for a Type 2 surveillance is detailed in Division 3, Part 3 of the 2006 Ordinance. It specifies that applications for authorization need to be submitted in writing by an officer of an authorized department[66] to the authorizing officer. Per the Ordinance, the head of an authorized department designates an officer, with the rank of Senior Superintendent of Police or higher, as the authorizing officer. The authorizing officer is empowered to either permit or refuse requests for executive authorization. The executive authorization remains valid for a maximum period of three months from the date of its approval.

A Commissioner was appointed under the 2006 Ordinance to review and ensure proper implementation of the Ordinance. Division 1, Part 4 of the Ordinance established the office of the Commissioner on Interception of Communications and Surveillance. The Chief Executive, in consultation with the Chief Justice, appoints a judge as a Commissioner for a period of three years.

Section 61 of the 2006 Ordinance — "Non-admissibility of telecommunications interception product" — prohibits the submission of intercepted information before any court or any person or the prosecution, except for verifying that a crime has been committed.

Until August 2006, the interception of telecommunications in Hong Kong was regulated by the Telecommunications Ordinance (Cap 106). Section 33 of the Telecommunications Ordinance, which contained the provisions for lawful interception of telecommunications, was enacted in 1963. According to this section the Chief Executive or any public officer authorized by the Chief Executive, could authorize the interception of communication. This occurred in circumstances where the Chief Executive believed that authorizing the intercept was in the "public interest".[67] The Ordinance neither enforced any limitation on the scope of an interception warrant (such as authorized methods of interception, offences that require interception of communication) nor did it specify the duration for the validity of warrants for interception. Moreover, the Ordinance did not contain any provision to prohibit the disclosure of the intercepted information.[68]

On June 27, 1997, the Interception of Communications Ordinance (Cap 532; IOCO) was passed. This Ordinance repealed Section 33 of the Telecommunications Ordinance. However, it has not come into effect as yet, primarily because neither the then-governor (prior to the handover of Hong Kong to China) nor the chief executive (since Hong Kong's handover) has appointed a date for its enforcement.[69]

62 Source: http://www.gld.gov.hk/egazette/pdf/20061024e/es12006102420.pdf
63 Source: http://www.info.gov.hk/gia/general/200501/26/lcq12_e.pdf , http://www.justice.org.uk/images/pdfs/JUSTICE
64 Source: http://www.hklii.org/hk/legis/ord/106/
65 List of authorized departments for covert surveillance is given under Part 2 of Schedule 1. The included departments are: Customs and Excise Department, Hong Kong Police Force, Immigrations Department and the Independent Commission against Corruption.
66 List of authorized departments for Type 2 surveillance is given under Part 1 of Schedule 1. The included departments are: Customs and Excise Department, Hong Kong Police Force and the Independent Commission against Corruption.
67 Source: http://www.hkhrm.org.hk/PR/Surveillance_All.doc
68 Source: http://www.legco.gov.hk/yr03-04/english/panels/se/papers/se0402ls-95-e.pdf
69 Source: http://legalref.judiciary.gov.hk/lrs/common/ju/ju_frame.jsp?DIS=53214&currpage=T

INDIA

Law Name	1. The Indian Telegraph Act, 1885 2. The Information Technology Act, 2000
Related Legislation	1. Indian Wireless Telegraphy Act, 1933 2. The Unlawful Activities Prevention Act, 1967 3. The Information Technology (Amendment) Bill, 2006 (Proposed) 4. Prevention of Terrorist Activities Act, 2002 (POTA)
Parties Responsible for Enforcing or Certifying	Union Home Secretary

In India, various laws have been passed to govern lawful interception. The Indian Telegraph Act, 1885 laid the country's foundation for lawful interception of communications. Subsequently, the Act was modified as the Indian Wireless Telegraphy Act, 1933. Other laws that followed were the Unlawful Activities Prevention Act, 1967, and the Information Technology Act, 2000. An amendment to the latter was proposed in 2006 and is known as the Information Technology (Amendment) Bill, 2006.

According to the Indian Telegraph Act, 1885, the word telegraph extended to all devices and instruments that could be used for the purpose of transmission of messages. It gave powers to the Indian government to intercept any form of telegraph during national emergency;[70] although it could only be done with the authorization of the central or state government. The Act was later modified in 1933 under the name of the Indian Wireless Telegraphy Act and was extended to wireless telegraphy equipment. The act also prohibited the general public from possessing a wireless transmission apparatus without a licence.[71] In 1967, the government passed the Unlawful Activities Prevention Act, which authorized police forces to use information obtained through interception of communication channels as evidence in trials.

The Telegraph Act, 1885, was further amended in 1996 by the Supreme Court, which ruled that wiretapping amounted to invasion of privacy, and was therefore a serious legal offence, unless conducted under appropriate guidelines. In the interest of national security and the issues related to law and order, the Supreme Court thus laid out clear guidelines for wiretapping, granting power of authorization to the Union Home Secretary in central government or his counterparts at the state level.

The Information Technology Act, the main act governing the interception of communication in cyber space, was passed by the Indian government in May 2000. Section 69 of the Act authorized law enforcement agencies to intercept any form of communication transmitted via a computer. Discretion for authorization in turn lies with the Controller of Certifying Authorities (CCA).[72]

In 2002, the Indian Parliament passed the Prevention of Terrorism Activities Act (POTA) that gave sweeping powers to law enforcement agencies to conduct interception of all communication channels being used for terrorist acts.

In 2001, a communications convergence bill was proposed in the Indian Parliament; it has not been passed by the house to date. If passed, it will give powers to the government or any officer to intercept a communication channel if required to do so in the interest of national safety or maintaining harmony with neighboring countries. It will also outline the penalties and punishments of telecom operators in the event of non-cooperation with law enforcement authorities.[73]

A proposal has also been made in Parliament for amendment of the Information Technology Act of 2000, known as the Information Technology (Amendment) Bill, 2006. It proposes to confirm the powers of the government to intercept and monitor any communication channel in the face of threats to national integrity and sovereignty and to oblige operators to aid law enforcement

agencies by providing them with access to computer resources and assistance in intercepting, monitoring, and decrypting any data suspected to be of critical nature — failing which, they would be punishable by law.[74]

70 Source : http://www.dot.gov.in/Acts/telegraphact.htm
71 Source : http://www.dot.gov.in/Acts/wirelessact.htm
72 Source : http://www.privacyinternational.org/survey/phr2003/countries/india.htm
73 Source : http://www.dot.gov.in/Acts/draftconvergence.pdf
74 Source : http://164.100.24.208/ls/bills-ls-rs/2006/96_2006.pdf

IRELAND

Law Name	Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993
Related Legislation	1. Postal and Telecommunications Services Act, 1983 2. Post Office (Amendment) Act, 1951 3. Official Secrets Act, 1963 4. The Criminal Justice (Terrorist Offences) Act, 2005
Parties Responsible for Enforcing or Certifying	1. Minister for Justice 2. Commissioner of the Garda Síochána

Passed as an amendment to the Postal and Telecommunications Services Act, 1983, the 'Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993'[75] is Ireland's legislation to govern lawful 'phone-tapping', 'wiretapping' and electronic surveillance.

This Act defines 'interception' and the process for legally intercepting both postal packets and telecommunications messages. For authorization, a written application must be sent to either the Commissioner of the Garda Síochána (Commissioner) or the Minister for Justice (Minister). This authorization is granted by the Minister or the Commissioner in cases of a threat to state security. In cases of exceptional urgency, this authorization can be given orally by the Minister, but needs to be substantiated into a warrant at the earliest opportunity. For cases pertaining to criminal investigations, the authorization is granted only by the Commissioner in the form of a warrant.

The warrant should include the date on which authorization is granted and the postal addresses of concerned parties, the type of proposed interception (postal packets, telecommunications messages or both), and the need for disclosure of intercepted materials. Under Sections 7 and 8 (6) of the Act, the warrant

remains in force for a period of not more than six months, but can be extended under the provisions provided in Subsection (6). Under Section 11 (1) of the Act, all official documents related to application and authorization must be retained for a minimum of three years from the date on which the warrant expires.

Section 110 of the Act makes it mandatory for telecom service providers to also retain data for 36 months. Similarly, the Criminal Justice (Terrorist Offences) Act 2005 states that all official documents including authorization and its application should be retained for at least three years at all fixed-line and mobile phone service providers from the date on which the authorization is enforced.[76]

The Freedom of Information Act, 1997[77] (FOI Act, 1997) enables the public to access the information held by government agecies. The information can include the intercepted telephone records of individuals. However, Section 32(1) (b) of the Act[78] grants permission to the government agencies to refuse an individual's request for disclosure of information regarding his/her intercepted telephone records. This is also in compliance with Section 12 of Act of 1993, which permits the non-disclosure of certain intercepted records of individuals.

The concept of interception of communications was embedded in the Postal and Telecommunications Services Act, 1983[79], Section 98, which prohibited the interception of telecommunication messages. It authorized members of the Garda Síochána to intercept telecommunication messages for a complaint received regarding suspected offences under Section 13 of the Post Office (Amendment) Act, 1951.[80] Such an interception could also be carried out after obtaining permission from the Minister under Section 110, of the Act of 1983.

75 Source: http://www.irishstatutebook.ie/ZZA10Y1993.html
76 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005greece-latvia.pdf
77 Source: http://www.finance.gov.ie/viewdoc.asp?DocID=837
78 Source: http://www.oic.gov.ie/en/DecisionsoftheCommissioner/LetterDecisions/Name,1037,en.htm
79 Source : http://www.irishstatutebook.ie/1983/en/act/pub/0024/index.html
80 Source: http://www.irishstatutebook.ie/ZZA17Y1951.html

ISRAEL

Law Name	The Secret Monitoring Law, 1979 Related Legislation The Computer Law, 1995
Related Legislation	The Computer Law, 1995
Parties Responsible for Enforcing or Certifying	1. President of the District Court 2. Chief Military Censor

The Secret Monitoring Law, passed in 1979, serves as Israel's primary interception legislation. This law permits the legal use of wiretapping and other means for intercepting communications.[81]

Under this law, Israeli police require permission from the President of the District Court before intercepting any form of wire or electronic communication. The law also permits the use of a microphone for interception. Warrants are issued for three months and can be renewed if required. The Chief Military Censor can also intercept cross-border or international calls to or from Israel for censorship purposes. In addition, intelligence agencies may wiretap suspects who potentially jeopardize national security, but only after receiving written permission from either the Prime Minister or Defence Minister.

The Secret Monitoring Law was amended in 1995 in view of findings filed by the State Comptroller, highlighting the abuse of wiretapping procedures by the police force; procedures were tightened accordingly. In addition, the amendment also widened the scope of the Act to cover new technologies such as mobile and Internet/PC communication, including e-mails. The collection of e-mail would be legal for targets who have been accused of a crime, but who have not been convicted to date. This modification in the law also increased the penalties for illegal wiretapping and permitted the interception of privileged communications, such as conversations with doctors, lawyers, etc. In turn, law enforce-

ment agencies must present an annual report that details all interception activities, to the Knesset (Israeli Parliament).

The Postal and Telegraph Censor, the civil department under the Ministry of Defence, has the authority to scrutinize any postal mail or courier in order to maintain civil order or national security. The Computer Law 1995 prohibits and penalizes unauthorized access to a computer.

According to official records, the number of wiretapping cases carried out by the police in 1999, 2000, and 2002 was 1,700, 1,685 and 1,089, respectively. The 2005 annual report by the police suggested that out of 1,095 requests by police for wiretapping, 1,089 were approved by the district court.[82]

81 Source: http://www.privacyinternational.org/survey/phr2003/countries/israel.htm
82 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005greece-latvia.pdf

ITALY

Law Name	Penal Procedure Code (Articles 266–271)
Related Legislation	1. Computer Crime Law, 1993 2. Act No.140 (2003) 3. Act No.45 (2004)
Parties Responsible for Enforcing or Certifying	1. Garante 2. Court

In Italy, lawful wiretapping is regulated by Articles 266 to 271 of the Penal Procedure Code.[83] This authorization is provided in cases pertaining to legal proceedings. These articles also include the types of communications which can be lawfully intercepted.

Prior to the interception of communication, a court approval is required. This approval lasts for 15 days, but can be renewed for a further 15 days if required. Intercept data (excluding location data) must also be retained for a period of 4 years, (increased from 30 months in February 2004 by Act No. 45/2004). The increased data retention period applies only to telephony traffic data. Location data on fixed line and mobile telephony must be retained for 29 months. Operators must also retain the records of all unsuccessful dial attempts. In addition, ISPs need to retain all data for at least six months.[84]

Judges monitor the procedures for recording and storing intercepted information. Any information which is not used is destroyed. However, conversations of religious ministers, doctors, lawyers, and other professionals that are categorized under professional confidentiality rules cannot be intercepted. Conversely, there are more lenient procedures for Anti-mafia cases when issuing a warrant for the interception of communications. In October 2001, the government reached a verdict on facilitating telephone tapping and electronic surveillance when considering serious offences, such as drug peddling, murder, etc. This practice only required the authorization and supervision of judicial authorities.

A report submitted in June 2002 indicated that Rome witnessed around 13,000 cases of legal wiretaps over a period of one year. According to some sources*, Italy is the world's most wiretapped country. In 1992, around 15,000 cases were authorized, and this had increased to 44,000 by 1996. The exponential increase in the number of legalized interceptions continued into the 21st century: In 2002, 2003, and 2004, the numbers of interception cases stood at 45,000, 77,000, and 100,000[85], respectively. The wiretapping cases increased three-fold from 32,000 in 2001 to 106,000 in 2005.[86]

*Based on 2002 statistics – 76 wiretaps per 100,000 inhabitants.[87] The main reason for this high level of wiretapping could be traced to an Italian law of 1992. This law allows wiretapping to be implemented on a per crime basis by order of a prosecutor, and does not require prior approval or supervision from judicial authorities. That said, the intercepted information cannot be used as evidence but can assist in the preparation of cases.

83 Source: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83522
84 Source: http://en.wikipedia.org/wiki/Data_retention
85 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005greece-latvia.pdf
86 Source: http://www.akdart.com/priv7.html
87 Source: http://www.edri.org/edrigram/number2.21/wiretaps

JAPAN

Law Name	Communications Interception Law, 1999
Related Legislation	None
Parties Responsible for Enforcing or Certifying	Court

The Communications Interception Law, 1999, governs lawful interception in Japan. Prior to the enforcement of this law, wiretapping was prohibited and considered illegal under Article 14 of Japan's Wire Telecommunications Law and Article 104 of Japan's Telecommunications Business Law, and a violation of the Constitutional Right of Privacy.[88]

The Communications Interception Law was passed by the Japanese legislative assembly (Diet) in August 1999, but it was enacted in August 2000 after several amendments. The law permits the law enforcement agencies (LEAs) to intercept communications on phone, fax, and the Internet in criminal cases involving organized murder, illicit firearms trade, drug trafficking, and smuggling of illegal immigrants into Japan. However, the communications of doctors, lawyers, and religious leaders cannot be intercepted under the law[89] and media communications can only be intercepted under certain conditions.[90] The law also directs ISPs to maintain a log of all the Internet communications that are monitored at any time.

According to the law, LEAs, which include prosecutors, police officers at the rank of superintendent and above, narcotic controllers, and Japan's Maritime Safety Agency officials, can execute wiretapping upon receipt of an authorized warrant. The warrants are issued by the district court judges for 10 days and can be extended up to thirty. The law also requires the presence of a third-party non-police witness, such as an employee of either the communication service provider or regional government, for monitoring the wiretapping process. In addition, LEAs are required to

notify individuals (whose communications have been intercepted) within 30 days of concluding the investigation and all documents pertaining to the communication must be destroyed thereafter.[91] To prevent the abuse of the law, spot monitoring (only some portions of communications can be intercepted and the process must terminate if the communication is considered to be innocent) is used for wiretapping. And in cases involving investigations by prosecutors, the court warrant is issued by a chief prosecutor, the head of the regional prosecutor's office.

The law does not define the devices or surveillance tools that can be used for lawful interception.[92] According to officials in the Ministry of Justice, only five authorized wiretaps were conducted in 2005, but the number is expected to increase considerably in the future.[93]

88 Source: http://www.csd.uwo.ca/~markp/htmls/Echelon2.pdf
89 Source: http://www.csd.uwo.ca/~markp/htmls/Echelon2.pdf
90 Source: http://www.snapshield.com/www_problems/Japan/Wiretap_but_carefully.htm
91 Source: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83523#_ftn22
92 Source: http://www.glo.org/?q=node/976
93 Source: http://search.japantimes.co.jp/cgi-bin/nn20070217a9.html

REPUBLIC OF KOREA

Law Name	Protection of Communications Secrets Act 1993
Related Legislation	None
Parties Responsible for Enforcing or Certifying	1. Police 2. High Court Judge

The Protection of Communications Secrets Act[94] 1993, also known as the Anti-Wiretap Law, regulates lawful interception in the Republic of Korea. This Act defines situations in which the government may intercept communications through telephone calls, post, mail, or other forms of communication. The intercepted information can be used as evidence in civil court or criminal cases.

According to this act, a government official — such as the prosecutor — needs to seek prior permission from a court for authorization to intercept communications. These applications for interception should be in writing and approved surveillances are usually conducted for two months in the case of criminal investigation. For issues relating to national security, the head of intelligence and investigative agencies must secure a warrant from the Senior Chief Judge of the High Court or an approval from the President. In these cases, surveillance periods of up to four months[95] may be granted. In all cases, applications for warrants should specify the reason for interception.

In November 1999, the Korean government proposed to amend the Protection of Communications Secrets Act (1993), which would allow victims of illegal wiretapping to bring charges against the government and thus curb the number of unauthorized wiretapping cases. In turn, the government established a 'wiretapping complaint center' under the Ministry of Information and Communication (MIC) in 1999.

On November 9, 2004, a proposal was submitted by the government to the Korean National Assembly to amend the law regulating the privacy of communications. This proposed bill aimed to make it mandatory for investigating authorities to obtain an approval from a district court judge prior to tracking the location of a mobile phone user. In addition, the user must be made aware of this tracking within three months of providing the information to the governing authorities.[96]

There were 2,884 wiretapping cases reported in Korea in 2001, reflecting a 21 percent increase from the year 2000.[97] The government departments had made a total of 270,584 requests (both call signalling and call content) for interception of telecommunication in 2001, reflecting a 66.8 percent increase over 2000. MIC carried out 528 wiretapping requests from January to June in 2006 compared to 550 cases in the same period in 2005.[98]

94 Source: www.ictparliament.org/CDTunisi/ict_compendium/paesi/corea/COR27.pdf
95 Source: http://www.state.gov/g/drl/rls/hrrpt/2006/78778.htm
96 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005peru-sril.pdf
97 Source: http://www.privacy.org/pi/issues/tapping/
98 Source: http://www.state.gov/g/drl/rls/hrrpt/2006/78778.htm

LITHUANIA

Law Name	Law on Operational Activities,1997
Related Legislation	1. Law on Telecommunications,1998 2. Law on Electronic Communications, 2004
Parties Responsible for Enforcing or Certifying	1. Police 2. Special Investigation Service 3. Judge 4. Prosecutor General

The Lithuanian constitution and laws contain provisions that authorize the interception of communications. The Law on Operational Activities[99], enacted on June 10, 1997, serves as Lithuania's primary interception legislation. It also serves as the legal basis for carrying out overt and covert intelligence activities by law enforcement agencies, such as the police and the special investigation service. Other statutes with provisions for lawful intercept include the Law on Telecommunications[100], enacted on August 1, 1998; and the Law on Electronic Communications[101], enacted on May 1, 2004. As specified in these laws, lawful intercept is permitted for the purposes of protecting state secrets, preventing crime and detecting criminal acts.

The Law on Operational Activities obligates TSPs to assist LEAs in the successfull interception of information transmitted over their networks. Article 10 of the law details the provisions for implementing covert surveillance in the network and the procedure for obtaining information from TSPs. According to this article, authorization to monitor and record communications transmitted over telecommunication networks requires a warrant from a judge and the prosecutor general, or a prosecutor authorized by him. The application for authorization has to be submitted in writing to a regional court judge by the officer initiating the intercept. The authorization remains valid for a period of up to three months, after which it may be extended. The prosecutor

general or a person authorized by him is empowered to access all warrants issued for lawful intercept.

This same law also empowers LEAs to access historical telecommunication information stored at the TSPs. Paragraphs 12 and 13 of Article 10 define the procedure for LEAs to acquire such information. According to Paragraph 12, the judge of a district court, upon receipt of an application from the head of the concerned LEA or authorized deputy, can provide authorization to obtain such information. Paragraph 13 specifies that the LEA is required to provide a notice to the TSP requesting their assistance in interception. This notice includes the application number, duration of intercept, date, and the name of the court that has issued the authorization.

The Law on Telecommunications carries additional obligations for the TSPs to assist the LEAs in carrying out lawful intercept. This law required the TSPs to retain data transmitted through telecommunication networks and make it available to the LEAs free of cost.[102] These data retention provisions, however, were never enforced as they were repealed by a ruling of the Constitutional Court on September 19, 2002.[103] According to the court's decision, the provisions for unlimited and unpaid data retention were unconstitutional. The court ruling also permitted the TSPs to choose the scope and length of retaining the data while complying with data protection laws.

Lithuania made efforts to align its laws with the EU directives of 2002 on electronic communications including the EU Directive on Privacy and Electronic Communications (2002/58/EC). As a result, the Law on Electronic Communications was enforced on May 1, 2004 after being enacted on April 15, 2004. From the date of enforcement of this new law, the Law on Telecommunications was rendered null and void. Currently, the operations of electronic communications in the country are regulated by the Law on Electronic Communications. This law regulates the processing

of personal data, defines provisions to maintain privacy in the electronic communications sector and contains provisions for communication intercept.

99 Source: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_e?p_id=268198&p_query=&p_tr2=
100 Source: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_e?p_id=192765&p_query=&p_tr2=
101 Source: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_e?p_id=242679&p_query=interception%20&p_tr2=2
102 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005lith-peru.pdf
103 Source: http://www.lrkt.lt/dokumentai/2002/r020919.htm

MALAYSIA

Law Name	Communications and Multimedia Act 1998
Related Legislation	1. Internal Security Act 2. Anti-Corruption Act 1997 3. Computer Crimes Act 1997 4. Criminal Procedure Code (Amendment) Act 2004
Parties Responsible for Enforcing or Certifying	1. Public Prosecutor 2. Royal Malaysia Police 3. Anti-Corruption Agency

The main legislation regulating the lawful interception of telecommunications in Malaysia is the Communications and Multimedia Act 1998.[104] Other statutes having provisions related to lawful intercept include the Internal Security Act 1960,[105] the Anti-Corruption Act 1997,[106] the Computer Crimes Act 1997,[107] and the Criminal Procedure Code (Amendment) Act 2004.[108]

The Communications and Multimedia Act (CMA) defines the provisions and procedures for intercepting communications, performing computer searches, accessing encryption keys, and other security related activities. Section 249 of the Act authorizes a police officer to search the content of a computer and request the disclosure information needed to access said content (password, encryption code, decryption code, etc.). Provisions for the interception of communications are listed under Section 252 of the CMA. It empowers the Public Prosecutor to authorize interception if it is believed that a particular communication will provide information important to the investigation of a crime under that falls under this Act or its ancillary legislation. A lawful intercept application needs to be submitted to the Public Prosecutor by an authorized officer or a police officer that is of the rank of Superintendent or above. In accordance with this section intercepted information is admissible as evidence against the accused during trial proceedings. The obligations for telecommunications service

providers (TSPs) are cited in Section 265. It obligates TSPs, as a part of their network license, to make their networks intercept capable for the LEAs.

Another piece of legislation which governs the interception of communications in Malaysia is The Anti-Corruption Act 1997. This act established the Anti-Corruption Agency which consists of a Director General and the members of the Agency. The provisions for intercepting communications are listed under Sub-section 38(4) of the Act. According to this sub-section, the Public Prosecutor may authorize the interception of communications upon receiving an application from an officer of the Agency with the rank of Superintendent and above. Permission for interception is only granted if the Public Prosecutor considers the intercepted information relevant to the court proceedings. If determined to be relevant, the intercepted information can be presented as evidence in court against the accused.

The Computer Crimes Act 1997 (CCA) defines provisions that prohibit unauthorized access to computers, data, programs and other electronic information. Section 10 of the Act empowers the Royal Malaysia Police to search, seize, and arrest criminals in the investigation of crimes under CCA. The Internal Security Act (ISA) also empowers the police to do searches, seize books and documents, intercept communications, and arrest offenders without a warrant.

The Criminal Procedure Code (CPC) was amended to expand the powers of the government to intercept telecommunications to prevent terrorist activities. Section 106c of the amended CPC empowered the Public Prosecutor to authorize the interception of communications for preventing terrorist acts. Similar to CMA, CCA, and the Anti-Corruption Act, the 2004 amendment of CPC also permits intercepted information to be used as evidence in court.

104 Source: http://www.commonlii.org/my/legis/consol_act/cama1998289/
105 Source: http://www.anfrel.org/mission_data/ISA%20-%20Malaysia.pdf
106 Source: http://politikus.xparte.com/aca1997.pdf
107 Source: http://www.commonlii.org/my/legis/consol_act/cca1997185/
108 Source : http://www.parlimen.gov.my/billindex/pdf/DR162004E(1).pdf

THE NETHERLANDS

Law Name	1. Code of Criminal Proceedings 2. Telecommunications Act, 1998
Related Legislation	1. The Special Investigation Powers Act, 2000 2. Intelligence and Security Services Act, 2002 3. Vorderen gegevens telecommunicatie, 2004 4. Functional Specification for lawful interception of Internet traffic in the Netherlands 5. Transport of Intercepted IP Traffic
Parties Responsible for Enforcing or Certifying	1. Court 2. Ministry of Interior 3. Minister of Economic Affairs 4. Minister of Justice

In the Netherlands, there are a number of laws governing the lawful interception of telecommunications including the Code of Criminal Proceedings (Wetboek van Strafvordering), Telecommunications Act (Telecommunicatiewet or TW) October 19, 1998, The Special Investigation Powers Act[109] or 'Wet BOB' (Wet Bijzondere OpsporingsBevoegdheden) February 1, 2000, and the Intelligence and Security Services Act[110] (Wet Inlichtingen en Veiligheidsdiensten), February 7, 2002.[111]

In addition to wiretapping, the interception of telecommunications extends to publicly available Internet services such as e-mails, chat, and web surfing. A warrant authorization is required before wiretapping or interception procedures can commence. The interception of communications for investigation of criminal cases is authorized by a court and is granted under Article 125m of the Code of Criminal Proceedings.[112] Specifically, Articles 126m and 126t authorize content interception, while Articles 126n and 126u authorize traffic data interception. In contrast, intercept activities conducted by intelligence agencies are authorized by the Minister of Interior.

The Telecommunications Act (TW) lists specific obligations for telecommunication service and access providers. Under Article 13.1 Paragraph 1, telecommunication service providers can only offer commercial services if the associated networks are wiretap-enabled. Service providers are then obligated to assist LEAs in the lawful interception of communications under Article 13.2. Article 13.4 Paragraph 1 mandates that service providers share all the information (subscriber's number, address, city, type of service, etc.) required by LEAs for carrying out interception orders. In addition, the operators must store traffic data for at least three months for data analysis. Article 13.8 offers provisions under 'special circumstances' which permits an exemption from the wiretapping obligations. This exemption can be granted only by the Minister of Economic Affairs in consultation with the Minister of the Interior and the Minister of Justice. However, the 'special circumstances' are somewhat ambiguous as they do not define the circumstances which fall under this category.[113]

Under TW Article 13.6, telecommunication service providers must bear the installation, maintenance, and overhead costs for enabling network wiretap capabilities, while the government reimburses only the administrative and labor costs for transferring intercepted traffic to LEAs. A recent law, 'Vorderen gegevens telecommunicatie' enforced in September 2004, also authorizes the public prosecutor to request traffic data from telecommunication service providers, although this authorization may only be granted if conviction on the crime would result in punishment of at least four years imprisonment.

The Intelligence and Security Services Act authorizes LEAs to intercept, search and scan satellite communications. It also permits the intelligence agencies to retain the intercepted information for a maximum period of one year.

The Special Investigation Powers Act was incorporated in order to streamline investigation methods for criminal cases.

There are also two specifications for the lawful interception of Internet communications — Functional Specification for lawful interception of Internet traffic in the Netherlands,[114] or the WAI Functional Specification — and the Transport of Intercepted IP Traffic[115] (TIIT). The WAI Functional Specification applies specifically to IP and email interception, while TIIT provides details on the handover interfaces (to law enforcement).

According to a 2003 report by the German Max Planck Institute for Foreign and International Criminal Law, the Netherlands is the world's second-most wiretapped nation. The Netherlands has an average of 62 wiretaps per 100,000 inhabitants, after Italy with 76 wiretaps.[116]

109 Source: http://english.justitie.nl/images/Special%20powers%20of%20investigation%20act_tcm35-14199.pdf
110 Source: http://www.eerstekamer.nl/9324000/1/j9vvgh5ihkk7kof/vg4nel1rvb0h/f=x.pdf
111 Source: http://wwwes.cs.utwente.nl/safe-nl/meetings/29-11-2002/lawful-intercept.pdf
112 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005lith-peru.pdf
113 Source: http://www.minez.nl/
114 Source: http://cryptome.org/nl-tap-specs.htm
115 Source: http://www.opentap.org/documents/TIIT-v0.1.2.pdf
116 Source: http://www.edri.org/edrigram/number2.21/wiretaps

NEW ZEALAND

Law Name	1. Telecommunications (Interception Capability) Act 2004 2. Government Communications Security Bureau Act 2003 3. International Terrorism (Emergency Powers) Act 1987 4. Misuse of Drugs Amendment Act 1978 5. New Zealand Security Intelligence Service Act 1969 6. Crimes Act 1961
Related Legislation	1. Crimes Amendment Act 2003 2. New Zealand Security Intelligence Service Amendment Act 1999 3. New Zealand Security Intelligence Service Amendment (No. 2) Act 1999
Parties Responsible for Enforcing or Certifying	1. Judge of a High Court 2. The Minister in charge of New Zealand Security Intelligence Service (NZSIS) 3. The Commissioner of Security Warrants

In New Zealand, the interception of telecommunication is governed by many laws including the Telecommunications (Interception Capability) Act 2004, Government Communications Security Bureau Act 2003, International Terrorism (Emergency Powers) Act 1987, Misuse of Drugs Amendment Act 1978, New Zealand Security Intelligence Service Act 1969, and Crimes Act 1961.

The Crimes Act 1961, Misuse of Drugs Amendment Act 1978, and International Terrorism (Emergency Powers) Act 1987 gave powers to the New Zealand police to intercept private communications under specific provisions; under the Crimes Act[117] the New Zealand police can use any interception device in criminal offence cases (including serious violent offences), subject to receiving an interception warrant signed by the Judge of the High Court. Likewise, the Misuse of Drugs Amendment Act 1978[118] permits the New Zealand police to intercept private communica-

tion — subject to a warrant authorized by a Judge of the High Court — in cases involving drug dealing and prescribed cannabis offences (cannabis on a substantial scale). The International Terrorism (Emergency Powers) Act 1987 permits the New Zealand police to intercept private communication during an emergency, again contingent on an authorized warrant[119]. Warrants are valid for no more than 30 days and all intercepted information must be destroyed after proceedings are complete.

The New Zealand Security Intelligence Service Act 1969[120], allows the New Zealand Security Intelligence Service (NZSIS) to carry out electronic interceptions upon issue of an intercept warrant by the Minister in charge of NZSIS and the Commissioner of Security Warrants. The Director of Security can apply for a warrant in cases of threats to national security and/or when needing to gather foreign intelligence information that is essential for security. The warrant is valid for a maximum period of 12 months. The Act was amended twice in 1999 (New Zealand Security Intelligence Service Amendment Act 1999 and New Zealand Security Intelligence Service Amendment (No. 2) Act 1999[121]), allowing NZSIS to install and maintain any equipment or device in the place under investigation and the issuance of foreign interception warrants (where the warrant is issued to intercept communications of a foreign organization or an individual who is neither a New Zealand citizen nor a permanent resident).[122]

Apart from the New Zealand police and NZSIS, the Government Communications Security Bureau (GCSB) — the Signals Intelligence (SIGINT) agency for New Zealand — has the power to intercept private communication and is responsible for both signals intelligence and communications security. The GCSB Act 2003[123] was enacted to specify the provisions by which GCSB can seek a warrant (or authorization for computer access) to protect the country's infrastructure from computer viruses and cyber threats by intercepting the communications of foreign organizations or persons.

The Telecommunications (Interception Capability) Act 2004[124] mandates that network operators and service providers assist surveillance agencies with the interception of telecommunications (phone call and e-mails), subject to an interception warrant from a High Court or under a lawful interception authority. The law ensures that the lawful interception of telecommunications is carried out effectively, and that network operators and service providers do not create any barriers to the introduction of advanced communication technologies. The surveillance agencies include law enforcement agencies (the New Zealand Police or any government department) or an intelligence and security agency (GCSB and Security Intelligence Service).

Deadlines for compliance were also set: For public switched telephone networks, or a telecommunications service, conformance is required within 18 months (the "lead time") from passing of the act; For public data networks, conformance is required within 5 years.

According to the law, network operators have to develop, install, and maintain interception capability across their public telecommunications networks and services. The network operator must also collect call-associated data and intercept telecommunications in a format specified by surveillance agencies (that can be decrypted by them). The operators must also ensure that the interception of telecommunications does not interfere with other communications services. The operators can adopt any network design features and specifications that are appropriate for their purposes.

During the nominated "lead time", costs incurred in developing, installing, and maintaining the interception facility are borne by the Crown in cases where the public switched telephone network or a telecommunications service has been operational before the date on which this Act was introduced as a bill into the House of Representatives (November 5, 2002); otherwise, costs are borne

by the network operator. After the expiration of the lead time, all costs are borne by the network operator. Reminder — the lead time refers to the period beginning from the introduction of the Bill into the House of Representatives and ending either 18 months later in the case of a public switched telephone network or a telecommunications service or five years later for a public data network.

The Telecommunications (Interception Capability) Act 2004 is similar to the US Communications Assistance for Law Enforcement Act (CALEA) 1994 and aligns New Zealand's interception capabilities and regulations with those in countries, such as Australia, the USA and the UK.

117 Source: http://www.legislation.govt.nz/libraries/contents/om_isapi.dll
118 Source: http://www.legislation.govt.nz/libraries/contents/om_isapi.dll?clientID
119 Source: http://www.legislation.govt.nz/libraries/contents
120 Source: http://www.legislation.govt.nz/libraries/contents
121 Source: http://www.legislation.govt.nz/libraries/contents
122 Source: http://www.privacyinternational.org/survey/phr2003/countries/newzealand.htm
123 Source: http://www.legislation.govt.nz/libraries/contents/om_isapi.dll?clientID=1606818175
124 Source: http://www.legislation.govt.nz/

NORWAY

Law Name	Criminal Procedure Act of 1981
Related Legislation	1. Criminal Code 1902 2. Postal and Telephonic Communications Act 1915 3. Telecommunications Act of 1995 4. Electronics Communication Act, 2003
Parties Responsible for Enforcing or Certifying	1. National Telephone Administration 2. Magistrate

In Norway, the Criminal Procedure Act, 1981, (lov om rettergangsmåten i straffesaker 22 mai 1981 nr 25) governs the lawful interception of telecommunications. Other laws that make provision for interception include the Criminal Code 1902, the Postal and Telephonic Communications Act 1915 (lov om kontroll med post- og telegrafforsendelser og med telefonsamtaler 24 juni 1915 nr 5), the Telecommunications Act of 1995 (Lov om telekommunikasjon), and the Electronics Communications Act 2003 (Lov om elektronisk kommunikasjon (ekomloven))[125].

According to the Criminal Procedure Act, wiretapping is permitted under a number of different circumstances. The first is detailed in section 216a which covers narcotics and national security offences. Section 216b covers provisions for wiretapping for less serious offences. In either case, the LEA needs to obtain a warrant from the magistrate court.[126] Under special circumstances, where the need for interception is urgent, section 216d grants that the prosecuting authority may issue an order in court. But subsequent approval for the order must be issued by the court within 24 hours of the warrant being granted.[127] Wiretaps in Norway have a statutory duration of four weeks while section 216f gives permission for a longer period of eight weeks if it is believed that intercepting the communications for four weeks will not be satisfactory. Section 216g mandates that the prosecuting

authority destroy all evidence collected through legal interception at the earliest, appropriate, opportunity.

The Criminal Code 1902 originally prohibited the interception of telephone networks except under special circumstances driven by criminal offences. Moreover, amendments to the Criminal Code prohibited individuals from examining electronic transmission. Later, the Postal and Telephonic Communications Act 1915[128] authorized the government to tap phone lines in cases concerning state security and narcotic drugs offences. The consent for tapping a phone line was provided by the National Telephone Administration.[129]

The Telecommunications Act of 1995 (under Section 9-3) prohibits communication network operators from releasing confidential and private data until an order is provided by the National Post and Telecommunications Authority. Section 7-2 obligates operators to provide unimpeded access to premises where telecommunication equipment is located, failure of which might result in cease and desist orders for telecommunication activity.[130] The Electronics Communication Act of 2003 reiterated the obligation of communication channel operators to maintain privacy of their electronic communications, until such prohibition is set aside by the necessary authorities (tribunal or magistrate) under formal circumstances.[131]

125 Source : http://www.lovdata.no/all/nl-20030704-083.html
126 Source : http://folk.uio.no/lee/publications/Overview_Butterworths.pdf
127 Source : http://www.ub.uio.no/ujur/ulovdata/lov-19810522-025-eng.pdf
128 Source: http://www.ub.uio.no/ujur/ulovdata/lov-19150624-005-eng.pdf
129 Source : http://www.afin.uio.no/forskning/andre_publikasjoner/schengen.pdf
130 Source : http://www.medialaw.ru/laws/russian_laws/telecom/npa/6etr/norv.htm
131 Source : http://www.privacyinternational.org/survey/phr2003/countries/norway.htm

THE PHILIPPINES

Law Name	Republic Act No. 4200 (1965)
Related Legislation	Human Security Act of 2007
Parties Responsible for Enforcing or Certifying	Court

The Republic Act No. 4200, also known as the Anti Wiretapping Act,[132] is the law governing interception of communication in the Philippines. The Act, which came into existence in 1965, prohibits and penalizes wiretapping or interception of any form of communication without proper authorization from the court. Sections 1–4 of the Act cover all aspects of lawfully intercepting communications.

Section 1 of the Act, states that it is unlawful to wiretap or intercept any form of communication, with any device or arrangement, or for any unauthorized person to intentionally possess any record of such communication, unless it is lawfully acquired as evidence for a criminal or civil trial.

Section 2 of the Act assesses the liability of a person who violates the provisions of Section 1. The person is subjected to not less than six months (and no more than six years) of imprisonment. In case the offender is a public official, he/she would be permanently dismissed from government office. In case the offender is an alien, he/she would be subjected to deportation proceedings.

According to Section 3 of the Act, any peace officer, with a written approval/order from the court, can execute wiretapping or possess records of intercepted communications, provided that the identity of the concerned parties and the officer is established and that there are reasonable grounds to prove that the crime has been committed, or is being committed. The reasonable grounds include "the crimes of treason, espionage, provoking war, and disloyalty in case of war, piracy, mutiny in the high seas,

rebellion, conspiracy and proposal to commit rebellion, inciting to rebellion, sedition, conspiracy to commit sedition, inciting to sedition, kidnapping as defined by the Revised Penal Code, and violations of Commonwealth Act No. 616, punishing espionage, and other offenses against national security"[133].

Section 4 of the Act states that any communication/information obtained through violation of the Republic Act No. 4200 shall not be admissible as evidence in any court hearing or investigation.

The Human Security Act of 2007, also known as the Anti-Terrorism Bill (ATB), was passed by the Senate on February 8, 2007, granting power to the government to intercept communications of terrorists. Section 7 of the Act legalizes the surveillance of suspected terrorists and gives authorities the power to intercept or record any communication.[134] Although there are stringent rules and regulations for prohibiting wiretapping, illegal wiretapping continues to remain a problem, and the cases pertaining to wiretapping are constantly increasing across the country.[135]

132 Source: http://www.chanrobles.com/republicactno4200.htm
133 Source: http://www.chanrobles.com/republicactno4200.htm
134 Source: http://www.bulatlat.com/statements/7-3/7-3-atb.htm
135 Source: http://www.privacyinternational.org/survey/phr2003/countries/philippines.htm

POLAND

Law Name	Code of Criminal Procedure, 1997
Related Legislation	1. Police Code 2. Ministerial draft regulation, 2001 3. Polish Executive Regulation, 2003 4. Telecommunication Act, 2004
Parties Responsible for Enforcing or Certifying	1. Minister of Justice 2. Minister of Interior 3. Court 4. Police

The Code of Criminal Procedure[136], enacted on 6 June 1997, regulates electronic surveillance/wiretapping in Poland. The initial provisions for wiretapping were laid out in the Criminal Procedure Code of 1982.[137]

Under Article 237 (1) of the Code of Criminal Procedure,[138] the police and intelligence services must receive approval from the court before carrying out wiretaps. This authorization may also be provided by the court upon receiving an application from the state prosecutor. The law also specifies those cases in which interception of communications is legal and includes such activities as homicide, kidnapping, hijacking, etc. In cases of exceptional urgency, the state prosecutor may authorize an interception, but the prosecutor is obligated to obtain an authorization from the court within five days. According to Article 238 (1), interceptions are authorized for three months and can be extended for a further three months at most. Courts order that all intercepted communication must be destroyed when it ceases to be of any significance to the criminal proceedings.

Telecommunication and postal service providers are obligated under Article 237 (5) of the Code of Criminal Procedure to ensure that an order for surveillance by the court or the state prosecutor is successfully implemented and such an interception is registered in their records. Only the court or the state prosecutor

is permitted to play the recordings of the interception except in urgent cases where the police, with permission from the court or the state prosecutor, may also play the recordings. The Ministerial Draft Regulation 2001 mandated that ISPs also be able to monitor all appropriate traffic. Moreover, the telecommunication service provider/operator is obligated under Article 165 of the Telecommunication Act[139] 2004, to store all transmission data for at least 12 months; after which this data is deleted or made anonymous.

The Polish Executive Regulation of February 22, 2003, mandates that telecommunications network operators provide access to the information which is transmitted through their telecommunications networks to state security agencies in order to maintain state security and public order.[140] The amendment which was initiated on March 18, 2004 was intended to align the Polish Criminal Code and the Criminal Procedure Code with the Council of Europe's Convention on cyber crime.[141]

136 Source: http://www.era.int/domains/corpus-juris/public_pdf/polish_ccp.pdf
137 Source: www.thepublicvoice.org/events/wroclaw04/adamski.ppt
138 Source: http://www.era.int/domains/corpus-juris/public_pdf/polish_ccp.pdf
139 Source: http://www.mt.gov.pl/viewattach.php/id/d4126689c59347e45b223648e31b10a6
140 Source: http://www.privacyinternational.org/survey/phr2003/countries/poland.htm#ftnref2128
141 Source: http://www.csirt-handbook.org.uk/

ROMANIA

Law Name	1. National Security Law, 1991 2. Police Organization Law, 1994
Related Legislation	1. Criminal Code 2. Law No. 41/1996 3. Law on Anti-Corruption No. 161/2003 4. Emergency Government Ordinance 131/2006, 2006
Parties Responsible for Enforcing or Certifying	1. General Prosecutor 2. Court 3. Serviciul Român de Informatii 4. Serviciul de Informatii Externe 5. Prosecutors Department for Investigations on Organized Crime and Terrorism

In Romania, the interception of postal and telecommunication messages is regulated by the National Security Law, enacted July 29, 1991 (Law No. 51/1991), and the Police Organization Law, dated May 12, 1994 (Law No. 26/1994).[142]

Article 13 of Law No. 51/1991 permits wiretapping in the case of crimes committed against the state. This is authorized by the General Prosecutor of the Office of the Supreme Court.[143] The authorization provided by the General Prosecutor has a maximum duration of six months with a possible extension of a further three months.

Conversely, the authorization granted in conventional criminal cases is limited to 30 days of surveillance. Under Article 17 of Law No. 26/1994, which defines the provisions for countering organized crime, the police can request the prosecutor's office to intercept calls and postal messages.

Article 14 paragraph 2 of Law No. 51/1991 states that the application for authorization has to be made in writing. The public prosecutor will only issue a warrant against the application if probable cause can be justified for the interception. In an

emergency, an intercept can be initiated without authorization, although authorization must subsequently be obtained within 48 hours. The Law also authorizes the Romanian domestic intelligence service, Serviciul Român de Informatii (SRI), and the Romanian foreign intelligence service, Serviciul de Informatii Externe (SIE), to carry out surveillance and interception.

Under Article 91 of the Criminal Code, recordings on magnetic tape could be used as evidence. In 1996, the Criminal Code was amended by passing Law No. 41/1996. This amendment introduced a new section related to the use and conditions under which audio or video recordings may be authorized.[144] Similar provisions for preventing cyber crimes were also introduced by the Law on Anti-Corruption No. 161/2003.[145]

In 2006, Romania adopted a new act — the Emergency Government Ordinance 131/2006 — which was eventually enforced on January 1, 2007, and increased the powers of the Department for Investigations on Organized Crime and Terrorism (DIICOT). According to the press and civil society groups, the prosecutors acting on behalf of the DIICOT will have the authority to monitor bank accounts and IT systems without a warrant. Naturally, the Ministry of Justice has been accused of breaching the right to privacy through this ordinance.[146]

142 Source: http://www.cdep.ro/legislatie/eng/vol42eng.pdf
143 Source: http://www.legi-internet.ro/index.php/Dreptul_la_viata_privata_si_Dr/123/0/?&L=2
144 Source: http://www.itu.int/ITU-D/e-strategies/e-legislation/Doc/Cybercrime_M_Menting.pdf
145 Source: http://www.coe.int/t/e/legal_affairs/legal_co-operation
146 Source: http://www.edri.org/edrigram/number5.2/romania-diicot

RUSSIA

Law Name	Federal Law on Operational-Search Activities, 1995
Related Legislation	1. Federal Law on Communications, 2004 2. Federal Law on Organs of the Federal Security Service in the Russian Federation, 1999 3. System for Operational-Investigative Activities, 1999 4. System for Operational-Investigative Activities, 1995
Parties Responsible for Enforcing or Certifying	1. Federal Security Service 2. Court of Justice 3. Court 4. Interior Ministry Police 5. Parliamentary and Presidential Security Guards 6. Border Patrol 7. Customs

In Russia, the interception of communications is primarily regulated by the Federal Law on Operational-Search Activities, 1995.[147] Other legislation with provisions for wiretapping and the lawful interception of telecommunications include the Federal Law on Communications, 2004[148]; Federal Law on Organs of the Federal Security Service in the Russian Federation,[149] 1995; System for Operational-Investigative Activities (SORM), 1995; and the System for Operational-Investigative Activities (SORM-2), 1999.[150]

The Federal Law on Operational-Search Activities empowers LEAs, such as the Federal Security Service, to intercept telecommunications (mobile phone communications, e-mails, etc.) for the purpose of detecting, preventing, and identifying criminals and criminal offences. All intercepted information relating to any person found not guilty must be destroyed. Article 5 of the law

also obligates the LEAs to destroy intercepted information within six months of the date on which the interception ceased.

According to Article 8 of the Federal Law on Operational-Search Activities, the interception of communications requires approval from a court. Under this article intercepted telephone conversations are admissible as evidence in criminal proceedings. Article 9 of the law states that court authorizations are valid for up to a maximum of six months from the date of their enforcement. A judge can extend the authorization further through a court ruling. This law was amended in 1999 and it extended the authority to perform lawful intercept to the Interior Ministry Police, the Parliamentary and Presidential security guards, the Border Patrol, Customs.

Provisions for lawfully intercepting communications are also defined under the Law on Communications, 2004. Article 63 and Article 64 of this law defines provisions for both performing lawful intercept and the obligations of telecommunication service providers (TSPs). According to Article 63, prior authorization from the Court of Justice is required for intercepting communications. Article 64 obligates TSPs to provide assistance to LEAs including providing subscriber information and implementing measures to facilitate the interception of communications.

The Federal Security Service (FSB) was established by the 1995 Federal Law On Organs of the Federal Security Service in the Russian Federation. Provisions for intercepting communications are defined in Article 9 of this law. It empowers the FSB to implement counter-intelligence activities including the interception of communications. Counter-intelligence measures are taken either in the investigation of serious crimes, such as drug trafficking and smuggling, or for the collection of intelligence information to protect the national security of Russia. All of these activities require prior approval from a court.

Russia introduced the System for Operational-Investigative Activities (SORM) legislation in 1995 to provide extensive powers to the FSB to monitor communications, e-mails, credit card transactions, Internet access and other electronic activities of users. In 1999, SORM-2 was introduced as an additional regulation to SORM, 1995. This new regulation defines the obligations of Internet service providers (ISPs) and the procedures the FSB must follow to monitor the Internet activity of users. ISPs are required to install equipment at their own expense to assist FSB in monitoring Internet traffic. The equipment is required to reroute, in real-time, all ISP data (incoming and outgoing) to FSB headquarters. Thus, this new legislation authorizes FSB to monitor Internet activity of all subscribers across all ISPs. In addition, ISPs are obligated to train FSB officials on the use of the equipment for the purpose of interception. However even though the information is routed to the FSB, the law requires the FSB to obtain court authorization before accessing any of the data received from the ISPs.[151]

147 Source: http://www.legislationline.org/legislation.php?tid=155&lid=6005&less=false
148 Source: http://english.minsvyaz.ru/docs/FED.doc
149 Source: http://www.fas.org/irp/world/russia/docs/law_950403.htm
150 Source: http://www.libertarium.ru/libertarium/37988, http://www.lenta.ru/internet/2000/08/21/sorm/, http://www.motherjones.com/news/
151 Source: http://mail.v2.nl/, http://lists101.his.com/pipermail/, http://www.cvni.net

SINGAPORE

Law Name	Computer Misuse Act, 1993
Related Legislation	1. Criminal Procedure Code 2. Internal Security Act, 1960 3. Electronic Transactions Act, 1998 4. Telecommunications Act, 1999 5. Statutes (Miscellaneous Amendments) Act 2005
Parties Responsible for Enforcing or Certifying	1. Police 2. Minister 3. Judge 4. Public Prosecutor 5. Controller of Certification Authorities

The main statute that regulates lawful interception of telecommunications in Singapore is the Computer Misuse Act, 1993.[152] Other legislation that contains provisions that authorize LEAs to access computers, seize documents, and intercept conversations include the Criminal Procedure Code[153], the Internal Security Act, 1960[154], the Electronic Transactions Act, 1998[155], the Telecommunications Act, 1999[156], and the Statutes (Miscellaneous Amendments) Act 2005[157].

Unauthorized interception of computer-based communications is prohibited under the Computer Misuse Act (CMA) of 1993. Under Part II of this Act, unauthorized interception of computer services may lead to a maximum fine of USD 20,000, imprisonment of up to 5 years, or both. Provisions that empower the police to intercept communications were listed under Section 15 of the 1993 Act. However, they were repealed through the Statutes (Miscellaneous Amendments) Act 2005. Subsequent to them being repealed, two new sections, 125A and 125B, were added to the Criminal Procedure Code (CPC) to redefine the LEA's powers.

According to Section 125A of the CPC, a police officer or an officer authorized by the Commissioner of Police in writing can intercept communications and access/search computers for

relevant information. This section also obligates all concerned persons to cooperate with the LEAs in performing their duties.

Section 125B of the CPC empowers the LEAs to decrypt any encrypted information. To achieve this, the Public Prosecutor authorizes a police officer or an officer with a prior written authorization of the Commissioner of Police to access the information or technology required to convert the encrypted information into a readable format. This section also requires all persons involved to assist LEAs in decrypting information deemed significant to the investigation.

The provisions to protect the confidentiality of conversations, documents, books, etc., have been defined under the Electronic Transactions Act (ETA). The Act established the Controller of Certification Authorities to ensure proper implementation of the Act. This Act defines provisions for the lawful interception of communications. Under Section 53, the Controller or an officer authorized in writing by the Controller can lawfully access computers and data, with persons related to the investigation obligated to assist the LEAs. Section 55 further empowered the Controller to request the production of documents, accounts, data, etc., from the concerned parties.

The Telecommunications Act, 1999 regulates the availability and application of equipment used for the interception of communications.[158] The provisions for lawful interception of telecommunications have been listed in Section 42, Part VI of the 1999 Act. Prior authorization from a court or a Minister is required to intercept any form of telecommunication, such as audio, e-mail, image, etc. In addition, the Internal Security Act authorizes the interception of communications for the purpose of safeguarding the national interests and security of Singapore.[159] The Act enables the government to conduct searches and intercept communications without a warrant.

152 Source: http://agcvldb4.agc.gov.sg/non_version/html/homepage.html
153 Source: http://agcvldb4.agc.gov.sg/non_version/cgi-bin
154 Source: http://agcvldb4.agc.gov.sg/non_version/cgi-bin
155 Source: http://agcvldb4.agc.gov.sg/non_version/cgi-bin
156 Source: http://app.supremecourt.gov.sg/data/doc/
157 Source: http://www.bakerinfo.com/apec/singapec_main.htm#Privacy
158 Source: http://www.civdialogue.asef.org/documents/BriefingPaper_002.pd
159 Source:

SOUTH AFRICA

Law Name	Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002
Related Legislation	1. Interception and Monitoring Prohibition Act, 1992 2. Interception and Monitoring Prohibition Amendment Act, 1995
Parties Responsible for Enforcing or Certifying	1. South African Police Service 2. Designated Judge

South Africa's Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002,[160] regulates the government's interception and monitoring of communications. This law was enacted in December 2002[161] — before this time, the Interception and Monitoring Prohibition Act (1992) governed all aspects of lawful interception. The latter permitted the interception and monitoring of communications and also facilitated the interception of postal articles in cases pertaining to serious crimes or the security of the South African Republic. The legislation was later amended in 1995 under the Interception and Monitoring Prohibition Amendment Act, 1995[162]. A further bill was introduced in the South African Parliament on July 18, 2001 proposing that the Interception and Monitoring Prohibition Act, 1992[163] be repealed and replaced. As a result, the 2002 Act came into existence[164].

The 2002 Act permits the interception and monitoring of certain communications including cellular phones and Internet applications via ISPs. In addition, this law clarifies the procedure for filing an application and issuing a warrant for interception.

The Act also describes the duties of telecommunication service providers (TSPs) and their customers. Chapter 5 of the Law states that all telecommunications service providers, including ISPs, need to make their networks capable of performing interception.

TSPs are required to bear the costs of deploying these capabilities. Criminal penalties may also be brought on service providers that do not comply with the provisions of the Act or do not assist the law enforcement authorities. In addition, TSPs must retain the communications-related data of their subscribers for at least 12 months, with this information being made available to the law enforcement authorities on request.[165]

The interception permit is provided in the form of a warrant issued by a designated judge in response to a written application. This application needs to have an internal departmental approval before application is made to the designated judge. In the case of the South African Police Service, approval is granted by an official who is an Assistant Commissioner or an official of the same rank. In the case of the South African National Defense, the internal approval is provided by an officer rank of Major General. Authorized warrants are valid for a maximum of three months. For cases of exceptional urgency, the application and the authority for interception can be given verbally.

In February 2000, the National Intelligence Agency (NIA) proposed the establishment of a signals intelligence service. This would provide NIA with the authority to intercept all forms of postal, telephone, and Internet communications for the purpose of detecting and preventing criminal offences and strengthening national security. In January 2004, the Department of Communications invited suggestions from technology companies to create centers to assist the interception, monitoring, and storage of e-mail and mobile phone messages.

160 Source: http://www.info.gov.za/gazette/acts/2002/a70-02.pdf
161 Source: http://www.privacyinternational.org/survey/phr2003/countries/southafrica.htm
162 Source: http://www.info.gov.za/acts/1995/a77-95.pdf
163 Source: http://www.privacy.org/pi/countries/south_africa/sa-interception-act-1992.txt
164 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005peru-sril.pdf
165 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005peru-sril.pdf

SWEDEN

Law Name	1. Criminal Procedure Code 27:18 2. Criminal Procedure Code 27:19
Related Legislation	1. Bill 2002/2003:74 2. Act 1996:416 3. Law of Secret Camera Surveillance (Paragraph 1) 4. Telecommunications Act, 1993 5. International Legal Assistance in Criminal Matters Act, 2000 6. Electronic Communications Act, 2002
Parties Responsible for Enforcing or Certifying	1. Police 2. Prosecutor

In Sweden, lawful wiretapping and wire surveillance is regulated by the Criminal Procedure Code 27:18 and Criminal Procedure Code 27:19, respectively. Wiretapping is defined as the interception of communication through telephone or fax. Wire surveillance is defined as the gathering of information regarding the number of messages sent from or to a specific telephone number and its time and duration. Camera surveillance is regulated in paragraph 1 of the Law of Secret Camera Surveillance and is used for investigative purposes.[166] Other statutes making provisions for lawful interception of telecommunications include the Telecommunications Act[167] (1993:597) of 1993, the International Legal Assistance in Criminal Matters Act[168] (2000:562) of 2000, and the Electronic Communications Act[169] (2002/03:110) of 2002.

Under the Criminal Procedure Code, the interception of communications is enforced by the police after obtaining a court order or warrant on the basis of a prosecutor's application. All permitted interceptions can only be used to aid the police in their investigations and for constructing a [prosecution] case. Telecommunication interceptions are valid from a minimum of 1 day to a maximum of 11 months, while camera surveillance usually lasts for no more than 29 days. Telecom operators are bound to

provide decrypted signals to authorities if required and to retain all traffic data generated through telephony or the Internet. The period of data retention may vary from a minimum of one year to a maximum of three years.[170]

In 1996, the Telecommunications Act was passed and obliged telecommunication service providers to maintain the privacy of the entire interception process while simultaneously providing the intercepted communication to law enforcement. The Telecommunications Act was eventually replaced by the Electronic Communications Act of 2002, which obligates all electronic networks and service providers to assist authorities with the process of wiretapping. This Act was eventually enforced on July 25, 2003.

The International Legal Assistance in the Criminal Matters Act makes provisions for the interception of communications of suspected criminals in Sweden and abroad. While the authorization for interception has to be provided by a prosecutor or a court, this Act also provides prosecutors with the authority to request legal assistance abroad. Chapter 4 (Sections 25–28) lists provisions for the interception of communications through wiretapping, telecommunications surveillance, and camera surveillance.

In 2003, the Swedish government approved Bill 2002/2003:74, which made it possible to lawfully intercept communications to investigate a number of crimes, such as murder, kidnapping, hijacking, etc. The new Act on Criminal Responsibility for Terrorist Crimes[171] also empowered the police to intercept and use secret surveillance techniques to monitor criminal behavior. This Act was enforced in July 2003.

New legislation has also been proposed due to increased incidents of crime and terrorism in Sweden. This legislation will offer the National Defence Radio Establishment (FRA) the authority to tap cross-border Internet traffic and phone calls without a court order. The law grants authorization to the police to use data min-

ing software to flush out data communications based on keyword search. However, communications within Sweden would not be affected by this legislation. If approved, the law will come into effect from July 1, 2007.[172]

During 1988 to 1996, the number of permitted wiretap cases ranged from 210 to 333.[173] In 2002, the number of cases increased to 533. Based on its relatively small population, Sweden was listed in third position with respect to the number of intercepts per inhabitants; in 2003, this ratio was 33 intercepts per 100,000 inhabitants. Only Italy and the Netherlands are ahead with 76 and 62 intercepts per 100,000 inhabitants, respectively.[174]

166 Source: http://www.ihf-hr.org/viewbinary/viewdocument.php?doc_id=5537
167 Source: http://www.medialaw.ru/laws/russian_laws/telecom/npa/6etr/swed.htm
168 Source: http://www.sweden.gov.se/content/1/c6/01/52/68/db667afc.pdf
169 Source: http://www.sweden.gov.se/content/1/c6/01/84/54/5ae98894.pdf , http://pts.se/Archive/Documents
170 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005swed-ven.pdf
171 Source: http://www.isp.se/documents/public/se/pdf/lagar/2003_148e.pdf
172 Source: http://cybrinth.com/uploads/031407%20Plain.doc
173 Source: http://cryptome.org/se-crypto99.htm
174 Source: http://www.smartmobs.com/archive/2007/03/07/electronic_surv....html

THE UNITED KINGDOM

Law Name	Regulation of Investigatory Powers Act 2000
Related Legislation	1. The Interception of Communications Act of 1985 (Section 2) 2. The Interception of Communications Act of 1988 3. Police Act 1997 4. The Interception of Communications Act of 2001 5. The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 6. Wireless Telegraphy Act 1949
Parties Responsible for Enforcing or Certifying	1. Secretary of State 2. Interceptor

In the UK, Section 2 of the Interception of Communications Act of 1985 laid the recognized foundation for lawful interception. This Act amended section 45 of the Telecommunications Act 1984. Three years later, the Act of 1985[175] was also modified so that it was in accordance with the Telecommunications (Interception) Act of 1979 of the Commonwealth. The modified Act, The Interception of Communications Act of 1988,[176] detailed the responsibilities of the police force, the office of police integrity, and special investigations monitoring. The Interception of Communications Act 2001[177] was a further modification of the 1985 version and dealt with issues encompassing the scope of warrants.

The Regulation of Investigatory Powers Act 2000[178] or RIPA is the primary legislation that now monitors and regulates the lawful interception of communications in the UK. It permits the Secretary of State to issue warrants authorizing the interception of postal services or a public telecommunications system in case of any threat to national security or for preventing or detecting criminal activities.

RIPA came into force on October 2, 2000 after the UK government realized the need for improved legislation to cover developing aspects of lawful interception. The new requirements were reflected in a consultation paper published in 1999. RIPA now describes the procedures of applying for and issuing a warrant. Only the heads of law enforcement agencies and their representatives are eligible to apply for interception warrants. These are then issued by the Secretary of State. The intercepted telephony data and subscriber information must be retained for 12 months while SMS, EMS, MMS, e-mail, and ISP data need only be retained for six.[179]

RIPA also describes the contents, duration, cancellation, and renewal requirements for warrants. Though the effective period of all new warrants is the same, it may vary if renewed. Of note, the tapped material cannot be used as legal evidence except under specific circumstances. RIPA also modified wiretapping to include all forms of telecommunications, vis-à-vis e-mails, chat, Web surfing, and Internet service, and made the tapping of private networks lawful as well. RIPA also empowered LEAs to serve notice to convert encrypted data to the readable or decrypted format; although this title has not been implemented at present.

The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002[180] defined the obligations of the public postal and public telecommunications service providers in accordance with RIPA. It was enforced on August 1, 2002. These obligations, however, do not apply to those telecom service providers who provide service to less than 10,000 people in the UK.

According to the provisions in the 2002 Order, telecom service providers need to enable an intercept within one working day of receiving a warrant. The service provider needs to ensure the completeness and near real-time transmission of intercepted data to the authorities. In addition, the transmission of both the intercepted and related communication data needs to be guaran-

teed. The handover interface needs to follow industry standards such as those prescribed by the European Telecommunications Standards Institute (ETSI).

The telecommunications service provider must only filter the traffic data for the target subscriber. In addition, the capability must exist for the simultaneous interception of 1 in every 10,000 subscribers. Moreover, the service provider needs to ensure that the reliability of the interception being carried out is at least equal to the telecommunication service which would be transmitting the intercepted communication. The interception capability can be audited; as a result, the premises are named in the warrant. The telecom service provider also needs to guarantee the secrecy of the intercept process.

The Interception Code of Practice[181] lays down the procedure that must be followed before the process of intercepting communication. The Police Act 1997[182], Part III, Section 92, makes provisions for intercepting wireless telegraphy while Section 93 deals with powers for authorization.

Under RIPA, 1,983 and 1,973 warrants for lawful interception were issued in 2003 and 2004, respectively, in England and Scotland. In addition, there were 3,367 modifications of warrants in 2004 as compared to 2,844 modifications in 2003.[183] Although the UK law enforcement agencies made 439,054 requests for communications data during January 2005-March 2006, only 2,407 requests were permitted for content-based lawful interceptions. In addition, there were 5,143 requests for modifications, aggregating the overall to 7,550.[184]

175 Source: http://www.swarb.co.uk/acts/1985InterceptionCommunicationsAct.shtml
176 Source: http://www.austlii.edu.au/au/legis/vic/consol_act/tpa1988556/
177 Source: www.gov.im/lib/docs/infocentre/acts/ica2001.pdf
178 Source: http://www.opsi.gov.uk/Acts/acts2000/20000023.htm
179 Source: http://en.wikipedia.org/wiki/Data_retention
180 Source: http://www.opsi.gov.uk/SI/si2002/20021931.htm
181 Source: http://www.minez.nl/
182 Source: http://www.opsi.gov.uk/acts/acts1997/1997050.htm
183 Source: http://www.statewatch.org/news/2005/nov/uk-tel-tap-rep-2004.htm
184 Source: http://www.statewatch.org/news/2007/feb/07uk-teltap-2005-2006.htm

THE USA

Law Name	1. Communications Assistance for Law Enforcement Act (CALEA): The law was introduced in 1994 2. Title II of USA Patriot Act, 2001 3. Foreign Intelligence Surveillance Act (FISA) of 1978 4. Title III of Omnibus Crime Control and Safe Streets Act of 1968
Related Legislation	1. The Wire and Electronic Communications Interception and Interception of Oral Communications Act 2. The Electronic Communications Privacy Act[185]
Compliance Deadlines	Communications Assistance for Law Enforcement Act (CALEA) • Original deadline of 25 October 1998 • Deadline extended to 30 June 2000 • Extension of deadline from 30 September 2001 to 19 November 2001 for CTIA[186] • ISPs compliance deadline of 14 May 2007[187]
Parties Responsible for Enforcing or Certifying	Predominantly, the FBI
Impacted Parties	Common carriers, facilities-based broadband Internet access providers, and providers of interconnected Voice over Internet Protocol (VoIP) service[188]

In the US, four main laws — the Communications Assistance for Law Enforcement Act (CALEA), Title II of USA Patriot Act of 2001, the Foreign Intelligence Surveillance Act (FISA) of 1978, and Title III of the Omnibus Crime Control and Safe Streets Act of 1968 — cover most of the nation's lawful interception statutes. While Title III of the Omnibus Crime Control and Safe Streets Act legislates lawful interception for domestic law enforcement purposes, the Foreign Intelligence Surveillance Act covers wiretapping for intelligence purposes where the subject could be a foreign (non-

US) person working as an agent on behalf of a foreign country. In 1994, the US Congress enacted CALEA to further clarify the statutory obligation of telecom carriers to maintain network infrastructures that assist law enforcement agencies with electronic surveillance. Moreover, post the 9/11 terrorist attack, Congress furthered electronic surveillance authorities under the USA PATRIOT Act. Provisions made under this act served mainly to broaden those already defined under FISA.

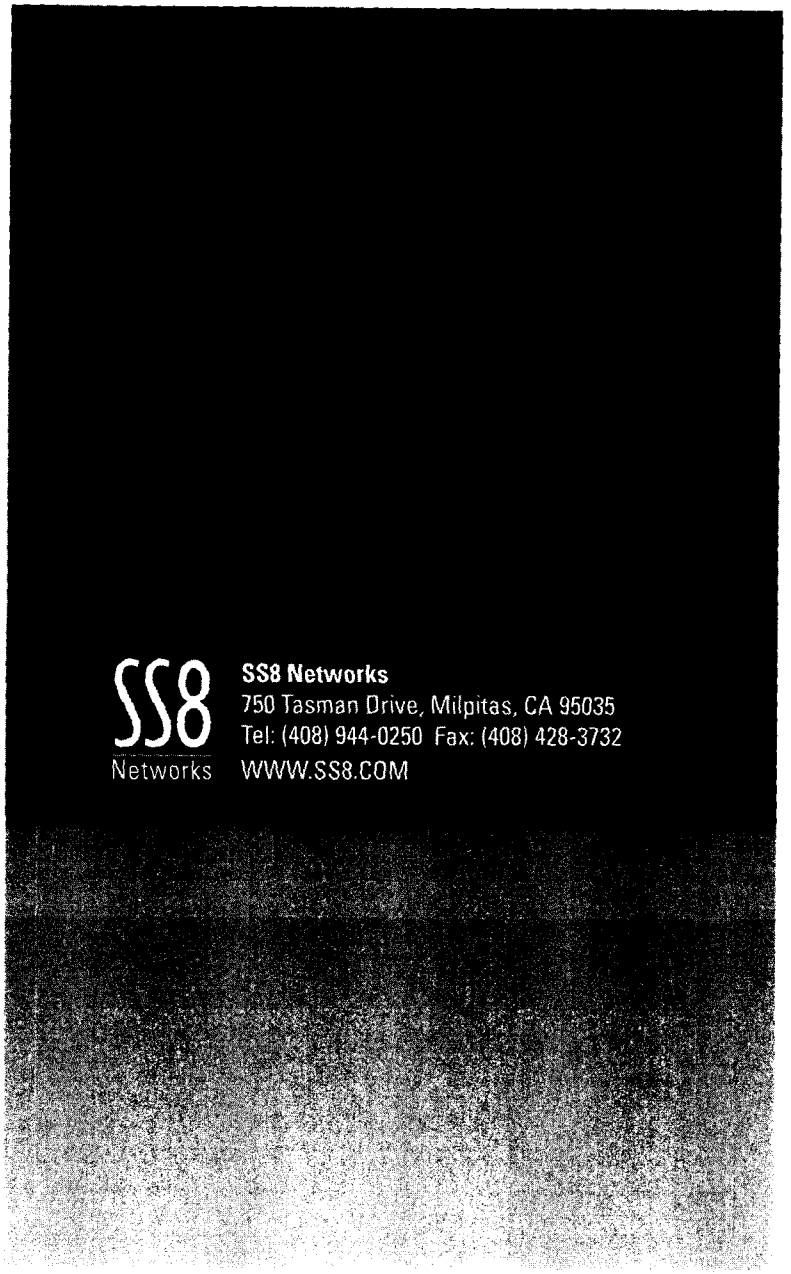
To guide carriers through the many laws covering legal interception in the US, telecom operators can look to CALEA as the legislation that most succinctly clarifies their obligations. The law was introduced in response to concerns that emerging technologies were creating difficulties for law enforcement agencies to execute authorized surveillance, and that a more standardized process was required.

According to the provisions of CALEA, a telecom carrier is required to design and maintain capabilities that allow customer traffic and signalling to be expeditiously and unobtrusively isolated, then forwarded to LEAs in a standardized manner to possibly multiple LEA locations (other than the premises of the carrier).[189] CALEA included a reimbursement clause, which allowed telecom operators to be repaid for the costs incurred in making their equipment, facilities, and services compliant with the requirements of CALEA if the equipment was installed pre-1995. A fund was set aside to support the upgrades of pre-1995 equipment, but the cost for post 1995 equipment compliance fell to the service provider.

The USA PATRIOT Act was a legislation milestone that significantly broadened the scope of federal electronic surveillance. The Act has added terrorist, computer fraud, and financial offences to the list of activities that can secure Title III wiretaps. The law also permits the use of roving wiretaps for foreign surveillance on US soil and expands the use of traditional pen register or

trap and trace devices from "call processing" to "the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications. Multi-jurisdictional warrants may also be obtained for wiretapping purposes, making it easier to track criminals across borders.[190]

185 Source: http://www.ncsl.org/programs/lis/CIP/surveillance.htm#Federal
186 Source : http://www.fcc.gov/Bureaus/Common_Carrier/Orders/2001/fcc01265.txt
187 Source : http://www.dslreports.com/shownews/83607
188 Source: http://www.fcc.gov/calea/
189 Source: http://en.wikisource.org/wiki/Communications_Assistance_for_Law_Enforcement_Act_of_1994
190 Source: http://www.fas.org/irp/crs/RL30465.pdf



McKinnon, Korey

From: Hawrylak, Maciek
Sent: October-15-12 4:22 PM
To: Scott, Marcie
Subject: Notes - Lawful Access - German Telecommunications Act 2004 - 2004-06-22
Attachments: PS-SP-#691109-R-Notes_-_Lawful_Access_-_German_Telecommunications_Act_2004_-_2004-06-22.PDF.DRF

German legislation.

Maciek

Telecommunications Act (TKG)*

of 22 June 2004

The German Bundestag, with the consent of the German Bundesrat, has adopted the following Act–

Contents

This Act serves to transpose the following Directives–

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33);
Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) (OJ L 108 page 21);
Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) (OJ L 108 page 7);
Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108 page 51); and
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 108 page 37).

Chapter 3
Rights of Way

PART 6
UNIVERSAL SERVICE

PART 7
PRIVACY OF TELECOMMUNICATIONS, DATA PROTECTION, PUBLIC SAFETY

Chapter 1
Privacy of Telecommunications

Chapter 2
Data Protection

Chapter 3
Public Safety

PART 8
REGULATORY AUTHORITY

Chapter 1
Organisation

Chapter 2
Powers

PART 1

GENERAL PROVISIONS

Section 1

Legislative Purpose

The purpose of this Act is, through technology-neutral regulation, to promote competition and efficient infrastructures in telecommunications and to guarantee appropriate and adequate services throughout the Federal Republic of Germany.

Section 2

Regulation and Aims

(1) Telecommunications regulation shall be under federal authority.

(2) The aims of regulation shall be–

1. to safeguard user, most notably consumer, interests in telecommunications and to safeguard telecommunications privacy;

2. to secure fair competition and to promote telecommunications markets with sustainable competition in services and networks and in associated facilities and services, in rural areas as well;

3. to encourage efficient investment in infrastructure and to promote innovation;

4. to promote development of the internal market of the European Union;

5. to ensure provision throughout the Federal Republic of Germany of basic telecommunications services (universal services) at affordable prices;

6. to promote telecommunications services in public institutions;

7. to secure efficient and interference-free use of frequencies, account also being taken of broadcasting interests;

8. to secure efficient use of numbering resources;

9. to protect public safety interests.

(3) Unless this Act expressly makes definitive arrangements, the provisions of the Competition Act remain applicable. The duties and responsibilities of the cartel authorities remain unaffected.

(4) The sovereign rights of the Federal Minister of Defence remain unaffected.

(5) Broadcasting and comparable telemedia interests shall be taken into account. The provisions of the media legislation of the federal states remain unaffected.

Section 3

Definitions

For the purposes of this Act

1. "call" means a connection established by means of a publicly available telephone service, supporting two-way communication in real time;

2. "application programming interface" means the software interface between applications and the operating functions of digital television receivers;

3. "customer data" means the data of a subscriber collected for the purpose of establishing, framing the contents of, modifying or terminating a contract for telecommunications services;

4. "significant market power" ("SMP") of one or more undertakings is deemed present where the criteria laid down in section 11(1) sentences 3 to 5 apply;

5. "value added service" means a service which requires the collection and use of traffic data or location data beyond that which is necessary for the transmission or billing of a communication;

6. "service provider" means a person who, on a wholly or partly commercial basis,

   a) provides a telecommunications service, or

   b) contributes to the provision of such service;

7. "digital television receiver" means a television set with an integrated digital decoder or a digital decoder designed for connection to the television set for the use of digitally transmitted television signals which can be enriched with additional signals, including conditional access;

8. "end-user" means a legal entity or a natural person not operating a public telecommunications network or providing a publicly available telecommunications service;

9. "frequency usage" means any wanted emission or radiation of electromagnetic waves between 9 kHz and 3000 GHz for use by radio services or other applications of electromagnetic waves. Frequency usage for the purposes of this Act also means the routing of electromagnetic waves in and along conductors in respect of which free use as provided for by section 53(2) sentence 3 is not given;

10. "commercial provision of telecommunications services" means telecommunications offered to third parties on a sustained basis, with or without profit-making intent;

11. "customer cards" means cards through the agency of which telecommunications connections can be established and personal data collected;

12. "sustainable competitive market" means a market in which competition has been secured such that it continues even after sector-specific regulation has been withdrawn;

13. "numbers" means character sequences which in telecommunications networks serve the purpose of addressing;

14. "user" means a natural person using a telecommunications service for private or business purposes, without necessarily having subscribed to that service;

15. "public pay telephone" means a telephone available to the general public, for the use of which the means of payment may include coins and/or credit/debit cards and/or prepayment cards, including cards for use with dialling codes;

16. "public telephone network" means a telecommunications network used to provide publicly available telephone services and which, in addition, supports other services such as facsimile and data communications, and functional Internet access;

17. "publicly available telephone service" means a service available to the public for originating and receiving national and international calls, including a facility for making emergency calls; publicly available telephone service also includes the following services: provision of operator assistance, directory enquiry services, directories, provision of public pay telephones, provision of service under special terms and provision of non-geographic services;

18. "telephone number" means a number, the dialling of which in the public telephone service allows a connection to a specific destination to be set up;

19. "location data" means any data collected or used in a telecommunications network, indicating the geographic position of the terminal equipment of an end-user of a publicly available telecommunications service;

20. "subscriber" means a natural person or a legal entity who or which is party to a contract with a provider of telecommunications services for the supply of such services;

21. "local loop" means the physical circuit connecting the network termination point at the subscriber's to the main distribution frame or equivalent facility in public fixed telephone networks;

22. "telecommunications" means the technical process of sending, transmitting and receiving signals by means of telecommunications systems;

23. "telecommunications systems" means technical facilities or equipment capable of sending, transmitting, switching, receiving, steering or controlling electromagnetic or optical signals identifiable as messages;

24. "telecommunications services" means services normally provided for remuneration consisting in, or having as their principal feature, the conveyance of signals by means of telecommunications networks, and includes transmission services in networks used for broadcasting;

25. "telecommunications-based services" means services which do not invoke a service delivered in a different place or at a different time but whose content service is delivered in the course of the telecommunications connection;

26. "telecommunications lines" means underground or overhead telecommunications cable plant, including the associated switching and distribution equipment, poles and supports, cable chambers and ducts;

27. "telecommunications network" means transmission systems and, where applicable, switching and routing equipment and other resources in their entirety which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

28. "transmission path" means telecommunications systems in the form of cable or wireless links with the associated transmission equipment, as point-to-point or point-to-multipoint links with a given information throughput (bandwidth or bit rate), including their network terminations;

29. "undertaking" means the undertaking itself or affiliated undertakings within the meaning of section 36(2) and section 37(1) and (2) of the Competition Act;

30. "traffic data" means data collected, processed or used in the provision of a telecommunications service;

31. "effective competition" means the absence of significant market power within the meaning of section 11(1) sentences 3 to 5;

32. "access" means the provision of services and/or the making available of facilities to another undertaking, under defined conditions, for the purpose of providing telecommunications services;

33. "conditional access systems" means technical procedures and/or arrangements making the legitimate use of protected broadcasting programmes conditional upon subscription or individual authorisation;

34. "interconnection" means the access providing the physical and logical linking of public telecommunications networks for the purpose of enabling the users of one undertaking to communicate with users of the same or another undertaking or to make use of services provided by another undertaking; services may be provided by the parties concerned or by other parties that have access to the network. Interconnection is a special type of access implemented between public telecommunications network operators.

Section 4

International Reporting Requirements

Public telecommunications network operators and providers of publicly available telecommunications services shall provide the Regulatory Authority, upon request, with all such information as it requires to fulfil its reporting requirements in relation to the European Commission and other international bodies.

Section 5

Means of Publication

Publications and notifications which the Regulatory Authority is required to effect under this Act shall be placed in its Official Gazette and on its website, unless otherwise provided for. Technical directives are also to be published in the Regulatory Authority Official Gazette.

Section 6

Notification Requirement

(1) Any person operating a public telecommunications network on a profit-oriented basis or providing a publicly available telecommunications service on a profit-oriented basis shall notify the Regulatory Authority without undue delay of beginning to provide, of providing with differences or of ceasing to provide his activity and of any changes in his undertaking. Such notification requires written form.

(2) The notification shall include the information required to identify the operator or provider according to subsection (1), in particular the company register number, the address, a short description of the network or service being provided and the date on which provision of the activity is due to begin. The notification is to be made on a form prescribed and published by the Regulatory Authority.

(3) Upon request, the Regulatory Authority shall within a period of one week confirm that the notification according to subsection (2) is complete and certify that the undertaking has the rights granted by or under this Act.

(4) The Regulatory Authority shall at regular intervals publish a list of notified undertakings.

(5) Where it is clear that the activity has ceased and the Regulatory Authority has not been notified in writing of such cessation within a period of six months, the Regulatory Authority may establish ex officio that the activity has ceased to be provided.

Section 7

Structural Separation

Undertakings operating public telecommunications networks or providing publicly available telecommunications services and having special or exclusive rights within the European Union for the provision of services in other sectors shall be required

1. structurally to separate the activities associated with the making available of public telecommunications networks and the provision of publicly available telecommunications services; or

2. to keep separate accounts for the activities associated with the making available of public telecommunications networks or the provision of publicly available telecommunications services to the extent that would be required if these activities were carried out by legally independent undertakings, so as to identify all elements of cost and revenue of these activities, with the basis for their calculation and the detailed allocation methods used, including an itemised breakdown of fixed assets and structural costs.

Section 8

International Status

(1) Undertakings providing international telecommunications services or, under their service offer, operating radio equipment which may cause harmful interference to the radio services of other countries, are deemed recognised operating agencies within the meaning of the Constitution and the Convention of the International Telecommunication Union. These undertakings are subject to the obligations arising from the Constitution of the International Telecommunication Union.

(2) Under the provisions of the Constitution of the International Telecommunication Union undertakings providing international telecommunications services shall

1. give absolute priority to all telecommunications concerning safety of life at sea, on land, in the air or in space, as well as to epidemiological telecommunications of exceptional urgency of the World Health Organisation;

2. accord priority to government telecommunications over other telecommunications to the extent practicable upon specific request by the originator.

PART 2

MARKET REGULATION

Chapter 1

Market Regulation Procedures

Section 9

Principles

(1) Markets meeting the conditions of section 10 and shown by a market analysis according to section 11 not to be effectively competitive are subject to regulation in accordance with the provisions of this Part.

(2) Undertakings having significant market power ("SMP undertakings") in markets within the meaning of section 11 are subject to measures imposed by the Regulatory Authority in accordance with this Part.

(3) Section 18 remains unaffected.

Section 10

Market Definition

(1) The Regulatory Authority shall identify, for the first time without undue delay after the entry into force of this Act, the relevant product and geographic telecommunications markets warranting regulation in accordance with the provisions of this Part.

(2) Warranting regulation in accordance with the provisions of this Part are markets with high, non-transitory entry barriers of a structural or legal nature, markets which do not tend towards effective competition within the relevant time horizon and markets in respect of which the application of competition law alone would not adequately address the market failure(s) concerned. Such markets shall be identified by the Regulatory Authority within the limits of its power of interpretation. In doing so, it shall take the utmost account of the recommendation on relevant product and service markets which the Commission publishes under Article 15(1) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33), as amended.

(3) The Regulatory Authority shall, following the procedure set out in section 12, submit to the Commission its proposals for market definitions in all cases in which such definitions would affect trade between Member States.

Section 11

Market Analysis

(1) After identifying markets which, under section 10, warrant regulation in accordance with this Part, the Regulatory Authority shall determine whether there is effective competition in the market being analysed. Effective competition is deemed absent if one or more undertakings have significant market power in this market. An undertaking is deemed to have significant market power if, either individually or jointly with others, it enjoys a position equivalent to dominance, ie a position of economic strength affording it the power to behave to an appreciable extent independently of competitors and end-users. In determining whether there is effective competition, the Regulatory Authority shall take the utmost account of the criteria established by the Commission, published in the Commission guidelines on market analysis and the assessment of significant market power referred to in Article 15(2) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33), as amended. Where an undertaking has significant market power in a relevant market, it may also be deemed an SMP undertaking in a closely related relevant market identified in accordance with section 10(2) where the links between the two markets are such as to allow the market power held in one market to be leveraged into the other, thereby strengthening the overall market power of the undertaking.

(2) In the case of transnational markets within the area of application of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33), the Regulatory Authority shall determine whether significant market power within the meaning of subsection (1) is present together with the national regulatory authorities of the Member States comprised in these markets.

(3) The proposals for determinations according to subsections (1) and (2), including designations of SMP undertakings, shall be submitted to the Commission following the procedure set out in section 12 inasmuch as trade between Member States would be affected.

Section 12

Consultation and Consolidation Procedure

(1) The Regulatory Authority shall give interested parties the opportunity to make representations, within a fixed period, on the proposals referred to in sections 10 and 11. The consultation procedures and their outcomes shall be published by the Regulatory Authority. This does not affect protection of the trade and operating secrets of the parties concerned. For this purpose the Regulatory Authority shall establish a single information point through which all current consultations can be accessed.

(2) Where sections 10(3) and 11(3) provide for a submission, the following procedure applies–

1. After carrying out the consultation procedure according to subsection (1) the Regulatory Authority shall make the proposals referred to in sections 10 and 11 and the underlying reasoning available to the Commission and to the regulatory authorities of every other Member State at the same time, informing the Commission and the regulatory authorities of every other Member State accordingly. The Regulatory Authority may not give effect to the proposals referred to in sections 10 and 11 prior to the expiry of a period of one month or longer as determined under subsection (1).

2. The Regulatory Authority shall take the utmost account of the representations of the Commission and the other national regulatory authorities according to para 1. It shall communicate the resulting draft to the Commission.

3. Where a draft according to sections 10 and 11 identifies a relevant market which differs from those defined in the prevailing version of the recommendation on relevant product and service markets published by the Commission under Article 15(1) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33) or where such draft determines the extent to which one or more undertakings have significant market power in this market and where the Commission indicates within the representations period according to para 1 sentence 2 that the draft would create a barrier to the single market or has serious doubts as to its compatibility with Community law and, in particular, the objectives of Article 8 of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33), the Regulatory Authority shall not give effect to the proposals before the end of a further two months. Where the Commission takes a decision within this period requiring the Regulatory Authority to withdraw the draft, the Regulatory Authority is bound by such decision. It may again consult the parties concerned on the Commission's decision following the procedure set out in subsection (1). Where the Regulatory Authority wishes to accept the amendments proposed by the Commission, it shall amend the draft in accordance with the Commission's decision and submit the amended draft to the Commission. Otherwise it shall inform the Federal Ministry of Economics and Labour of the Commission's decision.

4. In exceptional circumstances where the Regulatory Authority considers there is an urgent need to act – in derogation of the procedure according to subsection (1) and paras 1 to 3 – in order to safeguard competition and protect user interests, it may adopt proportionate and provisional measures immediately. It shall without undue delay communicate such measures, with full reasons, to the Commission and the regulatory authorities of every other Member State. A decision by the Regulatory Authority to make such measures permanent or

to extend the time for which they are applicable is subject to the provisions of subsection (1) and paras 1 to 3.

Section 13

Remedies

(1) As far as the Regulatory Authority (by order) imposes, amends, maintains or withdraws obligations as referred to in sections 19, 20, 21, 24, 30, 39, 40 or 41(1) as a result of market analysis according to section 11, the procedure set out in section 12(1) and (2) paras 1, 2 and 4 applies accordingly inasmuch as the measure would affect trade between Member States. Undertakings affected are to be given an appropriate period of notice of the withdrawal of any such obligations. The procedure according to sentence 1 may be carried out by the Regulatory Authority together with or subsequent to the procedure set out in section 12. Sentences 1 and 2 likewise apply to obligations as referred to in section 18.

(2) In the case of section 11(2) the Regulatory Authority shall, in agreement with the national regulatory authorities concerned, determine those obligations which are to be fulfilled by the SMP undertaking(s). The procedure set out in section 12(1) and (2) paras 1, 2 and 4 applies accordingly.

(3) Decisions as referred to in sections 18, 19, 20, 21, 24, 30, 39, 40 and 41(1) are issued together with the outcomes of the procedures set out in sections 10 and 11 as a single administrative act.

Section 14

Review of Market Definitions and Analyses

(1) Where the Regulatory Authority becomes aware of facts warranting the assumption that the outcomes reached under sections 10 to 12 no longer reflect the market as it currently is or where the recommendation referred to in Article 15(1) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33) has been amended, the arrangements of sections 10 to 13 apply accordingly.

(2) Apart from the cases referred to in subsection (1) the Regulatory Authority shall submit every two years the findings of its review of market definitions according to section 10 and of market analyses according to section 11.

Section 15

Procedure For Other Relevant Measures

Apart from the cases referred to in sections 10, 11 and 13 the Regulatory Authority shall, in respect of all measures having a significant impact on the relevant market, follow the procedure set out in section 12(1) prior to taking a decision, unless this is otherwise regulated by law.

Chapter 2
Access Regulation

Section 16
Interconnection Agreements

Every public telecommunications network operator shall, upon request, undertake to make an interconnection offer to other public telecommunications network operators in order to secure user communication, the provision of telecommunications services and service interoperability throughout the Community.

Section 17
Confidentiality of Information

Information obtained from public network operators in the process of negotiating access or interconnection may be used solely for the purposes for which it was provided. Such information shall not be passed on to any other party, in particular other departments, subsidiaries or partners of the negotiating parties, for whom such information could provide a competitive advantage.

Section 18
Control of End-User Access

(1) The Regulatory Authority may, in justified cases, impose obligations on public telecommunications network operators controlling access to end-users and not having significant market power to interconnect, upon request, their networks with those of other public telecommunications network operators, as far as may be necessary to secure user communication, the provision of services and service interoperability. Additionally, the Regulatory Authority may impose further access obligations on public telecommunications network operators controlling access to end-users and not having significant market power as far as may be necessary to secure end-to-end connectivity.

(2) With a view to developing sustainable competition in the retail market the Regulatory Authority may require public telecommunications network operators controlling access to end-users not to treat particular requesting public telecommunications network operators differently, directly or indirectly, without objectively justifiable reason, from other requesting public telecommunications network operators with regard to the availability and billing of telecommunications services, of services according to section 78(2) paras 3 and 4 and of telecommunications-based services. Where the Regulatory Authority imposes obligations under sentence 1, section 42(4) applies accordingly.

(3) The measures set out in subsection (1) shall be objective, transparent and non-discriminatory. Section 21(1) sentence 2 and (4) apply accordingly.

Section 19

Prohibition on Discrimination

(1) The Regulatory Authority may impose obligations on a public telecommunications network operator with significant market power requiring access agreements to be based on objective criteria, to be transparent, to grant equally good access and to meet the requirements of fairness and reasonableness.

(2) Obligations of non-discrimination shall ensure, in particular, that the operator applies equivalent conditions in the same circumstances to other undertakings providing like services, and provides services and information to others under the same conditions and of the same quality as it provides for its own services or those of its subsidiaries or partners.

Section 20

Transparency Obligation

(1) The Regulatory Authority may impose an obligation on an SMP public telecommunications network operator to publish, for undertakings with access entitlements, all such information as is required for use of the relevant access services and/or facilities, in particular accounting information, information on technical specifications, network characteristics, terms and conditions of supply and use, and the charges payable.

(2) The Regulatory Authority is authorised to specify the information an SMP operator is to make available and in which form the information is to be made available, as far as this is proportionate.

Section 21

Access Obligations

(1) The Regulatory Authority may, upon request or on its own initiative, impose obligations on SMP public telecommunications network operators to grant other undertakings access, including unbundled access that properly reflects their requirements, in particular if otherwise, the development of a sustainable competitive downstream retail market would be hindered or this development would run counter to the interests of the end-users. In considering whether an access obligation is justified and proportionate to the regulatory aims according to section 2(2), the Regulatory Authority has to take into account, in particular, the following factors–

1. the technical and economic viability, having regard to the pace of market development, of using or installing alternative facilities, bearing in mind the nature and type of interconnection or access proposed;

2. the feasibility of providing the access proposed, in relation to the capacity available;

3. the initial investment by the facility owner, bearing in mind the risks involved in making the investment;

4. the need to secure competition in public telecommunications networks and publicly available telecommunications services in the long term, most notably by creating incentives for efficient investment in facilities which will secure more competition in the long term;

5. industrial property rights and intellectual property rights;

6. the provision of services that are available throughout Europe; and

7. whether already imposed obligations as referred to in this Part or non-mandated services available in and taken up by a large part of the market are sufficient to ensure the regulatory aims according to section 2(2).

(2) The Regulatory Authority may, having regard to subsection (1), require SMP public telecommunications network operators, amongst other things,

1. to grant access to specified network elements and/or facilities, including unbundled broadband access;

2. not to withdraw access to facilities;

3. to grant access on a wholesale basis to particular services offered by the operator as offered to end-users, for the purpose of resale by third parties in their own name and for their own account. In doing so, past and future investment in innovative services is to be taken into consideration;

4. to create the necessary prerequisites for the interoperability of end-to-end communication, including the provision of facilities for intelligent network services and roaming (enabling the use of other operators' mobile networks outside the coverage area of the requesting mobile operator, for the requesting operator's end-users);

5. to grant access to operational support systems or similar software systems required to secure fair competition in the provision of services, while ensuring the efficient use of existing facilities;

6. to allow, in meeting the access obligations imposed under this subsection or under subsection (3), the use of access services and facilities and cooperation between undertakings with access entitlements, unless an SMP operator shows in the given instance that, for technical reasons, such use or cooperation is not possible or is possible to a limited extent only;

7. to grant access to single billing services and to the acceptance or first-time collection of receivables in accordance with the following, as far as the bill-issuers have not entered into an agreement with the predominant part of the hence relevant market of the providers of publicly available telecommunications services to whom their access customers are able to connect, and to grant other providers who have not entered into such agreement non-discriminatory access to these services under the terms and conditions laid down in the agreement–

    a) End-users who have not agreed anything else with other providers of publicly available telecommunications services are to be issued a bill by the bill-issuer which, independently of the tariff structures, presents the charges for telecommunications services, for services according to section 78(2) para 3 and for telecommunications-based services from other providers taken via the network termination point of the end-user. This also applies to charges for authorisation codes transmitted during the telephone connection when these are concerned solely with services. Payment to the

bill-issuer of these charges is effected by means of a single bill for the whole of the service taken and for the charges payable to him.

b) A billing obligation cannot be imposed in respect of unmetered services within the meaning of subpara a) sentences 1 and 2 whose charges exceed 30 euros (10 euros from 1 January 2008), metered telecommunications-based services and services according to subpara a) sentence 2 with charges exceeding 2 euros per minute in each case or for any services for which authorisation is required. Nor can an obligation to handle complaints relating to services billed for third parties, to send reminders or to collect charges payable to third parties be imposed.

c) Customer data required for the purpose of handling complaints, sending reminders or collecting charges for services within the meaning of subpara a) sentences 1 and 2 are to be transmitted by the bill-issuer to providers of publicly available telecommunications services. Providers billing customers themselves for services within the meaning of subpara a) sentence 2 are, from 1 April 2005, to be provided by the bill-issuer with the customer data required.

d) Providers of publicly available telecommunications services have to ensure in relation to the bill-issuer that no data records for services for which billing is to be effected which are not in compliance with the legal provisions or with consumer protection legislation are transmitted to him. The bill-issuer is not responsible or liable for services billed on behalf of third parties.

e) In his reminders the bill-issuer has to include an insert, given prominence by the way it is printed, stating that the customer may pay not only the amount of the reminder, but also the original, possibly higher, amount to the bill-issuer with discharging effect.

(3) The Regulatory Authority should impose the following obligations under subsection (1) on SMP public telecommunications network operators–

1. the granting of fully unbundled access to the local loop and shared access to the local loop (provision of access to the local loop or to the local sub-loop in such manner as to enable use of the entire frequency spectrum of the twisted metallic pair);

2. the interconnection of telecommunications networks;

3. the granting of open access to technical interfaces, protocols and other key technologies essential for service interoperability and virtual network services;

4. the provision of colocation and other forms of facility sharing, including building, duct and mast sharing, and the granting, to the users or their agents, of access to these facilities at any time.

(4) Where an operator shows that use of the facility would endanger the maintenance of network integrity or the safety of network operations, the Regulatory Authority shall not impose the access obligation relating to the facility or shall impose the obligation in different form. The maintenance of network integrity and the safety of network operations are to be judged on the basis of objective standards.

Section 22

Access Agreements

(1) An SMP public telecommunications network operator in relation to whom an access obligation according to section 21 has been imposed is to submit to other undertakings requesting these services and facilities in order to provide telecommunications services themselves, without undue delay but in any case not later than three months after the access obligation has been imposed, an offer for such access.

(2) Access agreements concluded by an SMP public telecommunications network operator require written form.

(3) An SMP public telecommunications network operator shall submit to the Regulatory Authority agreements on access services and facilities to which he is party as a provider without undue delay after their conclusion. The Regulatory Authority shall publish the place in which and the hours during which an agreement according to sentence 1 is available for inspection to persons requesting access services and facilities.

Section 23

Reference Offer

(1) The Regulatory Authority should require an SMP public telecommunications network operator who is subject to an access obligation according to section 21 to publish, normally within three months, a reference offer for the access service and/or facility for which there is general demand. This decision may be issued together with a decision on the imposition of an access obligation according to section 21.

(2) Where an SMP public telecommunications network operator does not submit a reference offer, the Regulatory Authority shall identify the access services and/or facilities for which there is general demand. For this purpose the Regulatory Authority shall give actual and potential users of such services and facilities the opportunity to comment. It shall subsequently give the SMP operator the opportunity to comment on which of the services and facilities thus identified should, in his view, constitute part of a reference offer.

(3) The Regulatory Authority shall, having regard to the comments referred to in subsection (2), determine the access services the SMP operator has to provide and the access facilities the SMP operator has to make available in a reference offer. The Regulatory Authority shall request the operator to submit, within a specified period, a corresponding reference offer with terms and conditions of supply and use, including the rates. It may attach to this request requirements relating to particular conditions, most notably with regard to fairness, reasonableness and timeliness. The reference offer shall be sufficiently comprehensive to enable acceptance by all users without further negotiations. The above sentences also apply in the event of the SMP operator having submitted an inadequate reference offer.

(4) The Regulatory Authority shall check and, in the event of failure to comply with the requirements relating to particular conditions, most notably with regard to fairness, reasonableness and timeliness, amend the reference offers submitted. The Regulatory Authority generally determines a minimum duration for reference offers. The SMP operator shall notify the Regulatory Authority three months prior to the expiry of this minimum duration of any intended modifications to or cessation of the reference offer. The decisions referred to in subsections (3)

and (4) sentences 1 and 2 may be challenged in their entirety only. Sections 27 to 37 apply in respect of rates regulation.

(5) Where an access service or facility is already the subject matter of an access agreement according to section 22, the Regulatory Authority may oblige the SMP public telecommunications network operator to offer, on a non-discriminatory basis, this service or facility to other users as well, if general demand for such service or facility is likely to develop. This also applies to access services and facilities an SMP public telecommunications network operator has been obliged to provide or make available under an order according to section 25.

(6) The Regulatory Authority may oblige an SMP public telecommunications network operator to modify his reference offer if general demand has changed significantly. This may refer both to the services and facilities themselves and to the main conditions for their supply. Subsections (2) to (5) apply with regard to modifications to the reference offer.

(7) The operator is obliged to include the reference offer in his general terms and conditions.

Section 24

Accounting Separation

(1) The Regulatory Authority may require an SMP public telecommunications network operator to keep separate accounts for certain activities related to access services and facilities. In particular, the Regulatory Authority as a rule requires a vertically integrated undertaking to make its wholesale prices and its internal transfer prices transparent. This is to prevent, amongst other things, a breach of the prohibition on discrimination and unlawful cross-subsidies. The Regulatory Authority may specify the format to be used and the accounting method to be applied.

(2) The Regulatory Authority may require submission, in prescribed form, of the cost accounting and bookkeeping records referred to in subsection (1), including all related information and documents, upon request. The Regulatory Authority may publish such information in suitable form insofar as this would contribute to achieving the aims set out in section 2(2). In doing so it shall have regard to the provisions on the maintenance of trade and operating secrets.

Section 25

Regulatory Authority Orders

(1) Where an access agreement according to section 22 or an agreement on access services and facilities according to section 18 has not been brought about either wholly or in part and the conditions specified in this Act for imposing an obligation to grant access are given, the Regulatory Authority shall, after hearing the parties concerned, order access within a period of ten weeks from referral by one of the parties to the intended agreement. In cases which have to be specially justified the Regulatory Authority may, within the period referred to in sentence 1, extend the procedure to a maximum of four months.

(2) An order is permissible only insofar as and for as long as the parties concerned fail to reach an access or interconnection agreement.

(3) The referral according to subsection (1) shall be in written form; it shall be substantiated. In particular, the following is to be set out–

1. the precise content of the Regulatory Authority order;

2. when access was requested and for which concrete services and/or facilities;

3. that serious negotiations have been held or that the other party has declined to enter into any such negotiations;

4. the points on which agreement has not been reached; and

5. explanatory remarks on the technical feasibility of any specific technical measures requested.

The referral may be withdrawn until such time as the order is issued.

(4) For the purpose of achieving the aims set out in section 2(2) the Regulatory Authority may also open a case on its own initiative.

(5) The subject matter of such order may be any of the terms and conditions of an access agreement, or the rates. The Regulatory Authority may attach to such order conditions with regard to fairness, reasonableness and timeliness. Sections 27 to 38 apply in respect of determining the rates.

(6) Where both the terms and conditions of an access agreement and the rates payable for the services and/or facilities requested are disputed, the Regulatory Authority should take partial decisions with regard to the terms and conditions and to the rates. The periods referred to in subsection (1) apply to any partial decisions taken by the Regulatory Authority. The Regulatory Authority order may be challenged in its entirety only.

(7) Documents submitted in the course of proceedings are considered only if this does not compromise observance of the period specified in subsection (1).

(8) Operators affected shall follow a Regulatory Authority order without undue delay unless the Regulatory Authority has specified a period in the order for giving effect to the order. To enforce such order the Regulatory Authority may set a penalty not exceeding one million euros in accordance with the Administrative Enforcement Act.

Section 26

Publication

The Regulatory Authority shall, having regard to the maintenance of the trade and operating secrets of the undertakings concerned, publish measures taken under this Chapter.

Chapter 3
Rates Regulation

Subchapter 1
General Provisions

Section 27
Aim of Rates Regulation

(1) The aim of rates regulation is to prevent the anti-competitive exploitation of, hindrance to and discrimination of end-users and competitors as a result of the pricing measures of SMP undertakings.

(2) The Regulatory Authority shall take care that rates regulation measures in their entirety are coordinated (consistency requirement). In particular, the Regulatory Authority shall coordinate the timeframes and the content of its measures and consider whether each measure is proportionate to the aims according to section 2(2).

(3) The Regulatory Authority shall, insofar as broadcasting and comparable telemedia interests according to section 2(5) sentence 1 are concerned, inform the state media authority with competence accordingly and include it in proceedings initiated. Upon application by the state media authority the Regulatory Authority shall, with reference to this Act, look into the matter of initiating proceedings and ordering measures in accordance with the following provisions.

Section 28
Anti-Competitive Conduct by an SMP Undertaking in Levying and Agreeing Rates

(1) No SMP telecommunications service provider and no SMP public telecommunications network operator may abuse his position when levying and agreeing rates. Abuse is constituted, in particular, by the undertaking levying rates which

1. prevail solely as a result of his having significant market power in the particular telecommunications market;

2. considerably prejudice the competitive opportunities of other undertakings in a telecommunications market; or

3. create advantages for particular users in relation to other users of the same or similar telecommunications services,

unless it has been shown that the conduct referred to in paras 2 and 3 is objectively justified.

(2) Abuse within the meaning of subsection (1) para 2 is presumed where

1. the price for the service in question does not cover its long run incremental costs, including a reasonable return on capital employed;

2. the margin between the price the SMP public telecommunications operator charges competitors for an access service or facility and the corresponding retail price is not enough to enable an efficient undertaking to achieve a reasonable return on capital employed in the retail market (margin squeeze); or

3. an undertaking bundles its products in objectively unreasonable manner. In determining whether or not this is the case, the Regulatory Authority has to consider in particular whether efficient competitors of the SMP undertaking could offer the bundled product on comparable terms.

Section 29

Rates Regulation Orders

(1) The Regulatory Authority may, as part of or in preparation for rates regulation procedures, order that

1. it be provided by an SMP undertaking with detailed information on its service offer, on its current and expected sales, on its current and expected sales volumes and costs, on the foreseeable effects on both end-users and competitors and with such other documents and information as it deems necessary for the proper exercise of its rates regulation rights under this Act; and

2. an SMP undertaking structure its cost statements in such a way as enables the Regulatory Authority to obtain the data required for rates regulation under this Act.

In addition, the Regulatory Authority may order that the documents referred to in paras 1 and 2 be transmitted on data carrier. The undertaking has to provide an assurance of conformity with the written documents.

(2) The Regulatory Authority may impose obligations on an SMP undertaking with regard to cost accounting systems. In such case it may oblige the SMP undertaking to make a description of the compliant cost accounting system publicly available, showing at least the main categories under which costs are grouped and the rules used to allocate costs, provided it does not effect such publication itself. Compliance of the cost accounting system is verified by the Regulatory Authority; the Regulatory Authority may also charge an independent body with verification. A statement concerning compliance is published annually.

(3) The Regulatory Authority may, by separate decision, oblige an SMP undertaking to offer access on the basis of particular tariff systems and to apply particular cost recovery mechanisms as far as may be necessary to achieve the regulatory aims according to section 2(2). In imposing such obligations the Regulatory Authority has to ensure the promotion of economic efficiency and sustainable competition and maximum benefit to the end-user from such obligations. Where the Regulatory Authority takes a decision as referred to in sentence 1, the SMP provider has to submit a rates proposal within a period of two weeks. The Regulatory Authority shall take a decision within a period of four weeks of submission of the proposal or of expiry of the time limit.

(4) To enforce orders according to subsections (1) and (2) a penalty not exceeding one million euros may be set in accordance with the Administrative Enforcement Act.

(5) The Regulatory Authority may prescribe the form in which rates and changes in rates, including service specifications and other rates-related components, are to be published.

(6) The Regulatory Authority may also require undertakings not having significant market power to provide information as referred to in subsection (1) para 1 and proceed in accordance with subsection (4) where necessary for the proper exercise of rates regulation under this Part.

Subchapter 2

Regulation of Rates for Access Services and Facilities

Section 30

Rates Regulation

(1) Save as provided in the subsections below, the rates charged by an SMP public telecommunications network operator for access services and/or facilities mandated under section 21 are subject to approval by the Regulatory Authority in accordance with section 31. In derogation of sentence 1 the Regulatory Authority should subject such rates to ex post regulation in accordance with section 38(2) to (4) when

1. the operator does not also, at the same time, have significant market power in the retail market in which he is active;

2. significant market power has been determined after the entry into force of this Act without the operator having been designated by the Regulatory Authority as having dominance prior to the entry into force of this Act;

3. this measure is sufficient to achieve the regulatory aims according to section 2(2).

(2) In derogation of subsection (1) rates for access services according to section 21(2) para 7 are subject to ex post regulation in accordance with section 38(2) to (4). Regulation of these rates under this Act is ruled out where an agreement according to section 21(2) para 7 has come about or where services which the bill-issuer cannot be obliged to provide are concerned.

(3) Rates charged by an SMP public telecommunications network operator for access services or facilities not mandated under section 21 are subject to ex post regulation in accordance with section 38.

(4) Rates charged under obligations according to section 18 by an operator who controls access to end-users and who does not have significant market power are subject to ex post regulation. Section 38(2) to (4) apply accordingly.

(5) Charges levied by an SMP public telecommunications network operator for access on a wholesale basis to particular services offered by him for the purpose of resale by third parties in their own name and for their own account shall, in derogation of section 31(1), be calculated on a retail minus basis to allow an efficient provider of telecommunications services to achieve a reasonable return on capital employed in the retail market. The charges shall be equivalent to the costs of efficient service provision at least.

Section 31

Approval

(1) Rates which require approval under section 30(1) sentence 1 are eligible for approval when they do not exceed the costs of efficient service provision. In justified cases the Regulatory Authority may review eligibility in accordance with the comparable markets principle as set out in section 35(1) sentence 1 para 1.

(2) The costs of efficient service provision are derived from the long run incremental costs of providing the service and an appropriate mark-up for volume-neutral common costs, inclusive of a reasonable return on capital employed, as far as these costs are required to provide the service. Section 79 remains unaffected.

(3) Expenditure exceeding that referred to in subsection (2) is taken into account only insofar as and for as long as such expenditure derives from a legal obligation or the undertaking seeking approval demonstrates other proper justification for it. Where the Regulatory Authority, in examining the cost statements, deems essential components of the stated costs inefficient, it shall request the operator, without undue delay, to explain whether and to what extent these cost components constitute expenditure within the meaning of sentence 1.

(4) In determining a reasonable return on capital employed the Regulatory Authority takes into account, in particular, the following factors–

1. the capital structure of the regulated undertaking;

2. the situation in the national and international capital markets and the rating of the regulated undertaking in these markets;

3. the requirements concerning the return on equity capital employed, whereby the service-specific risks of equity capital employed may also be acknowledged; and

4. the long term stability of the economic environment, also with a view to the situation as regards competition in the telecommunications markets.

(5) Rates subject to approval charged by an SMP public telecommunications network operator for access services and facilities are to be submitted to the Regulatory Authority prior to their intended effective date, together with all such documents as are required for approval to be granted. Where approval has been granted for a limited period only, the submission has to be effected not later than ten weeks before such limited period expires.

(6) The Regulatory Authority may require the submission of rates proposals. Where such request is not met within one month of its having been received, the Regulatory Authority shall commence proceedings on its own initiative. The Regulatory Authority shall decide on rates proposals within a period of ten weeks of receiving the submission or of commencing own-initiative proceedings. In derogation of sentence 3 the Regulatory Authority should decide on rates proposals submitted under the procedure set out in section 34 within a period of two weeks.

Section 32

Forms of Approval

The Regulatory Authority shall approve rates

1. on the basis of the costs of efficient service provision for individual services; or

2. on the basis of the benchmarks prescribed by it for the average rate of change in the prices of a basket of combined services (price cap) in accordance with section 34.

Section 33

Cost Statements

(1) Together with any rates proposal according to section 31(5) or (6) the undertaking has to submit all such documents as are required to consider the submission, in particular–

1. current cost statements, to be made available on data carrier also;

2. detailed service specifications, including details of quality of service and the draft general terms and conditions; and

3. details of sales, sales volumes, the level of the different costs referred to in subsection (2) and the contribution margins, and the development of user structures for the service concerned for the two years prior to submission, for the year of submission and for the following two years.

(2) Cost statements according to subsection (1) para 1 comprise costs that can be directly allocated (direct costs) and costs that cannot be directly allocated (common costs). To be included, in particular, in the cost statements according to sentence 1 is an account of–

1. the input volumes on which cost accounting is based, the relevant prices, in each instance both separately and averaged, target and actual capacity utilisation in the documentation period; and

2. the method used to determine costs and investment values, and information on plausible keys for allocating costs to each of the undertaking's services individually.

(3) In addition, the undertaking has to submit, regularly at the beginning of every financial year, information on its total costs and on their allocation to cost centres and to the individual services (cost units), broken down into direct costs and common costs. Information relating to non-regulated services may be summarised.

(4) In the transparency and presentation of their data, the cost statements shall be such as to enable an examination by the Regulatory Authority, quantification of the costs of efficient service provision and a decision to be taken within the period referred to in section 31(6).

(5) Documents not submitted together with the proposal are taken into account only if observance of the time limits is not compromised by later submission. Any additional documents or information requested by the Regulatory Authority during proceedings need be taken into account only if submitted by the undertaking within a time limit set by the Regulatory Authority.

(6) The same cost accounting methods are to be applied by the undertaking for each rates proposal submitted.

(7) The powers referred to in section 29 remain unaffected.

Section 34

Price Cap

(1) The Regulatory Authority shall determine the content of the baskets. Access services may be combined in one and the same basket only when the level of competition for these services is not expected to differ significantly.

(2) The Regulatory Authority shall establish the initial rate level for the access services grouped in a basket. It shall proceed from any rates that have already been approved.

(3) The benchmarks for approval under section 32 para 2 encompass

1. the rate of price increases in the economy overall;

2. the expected rate of growth in productivity of the SMP operator; and

3. suitable secondary conditions for preventing abuse as set out in section 28.

(4) To be taken into account in the specification of benchmarks, in determination of the rate of growth in productivity in particular, is the relationship between the initial rate level and the cost of efficient service provision as set out in section 31(2).

(5) To be taken into account in the specification of benchmarks are the rates of growth in productivity of undertakings in comparable competitive markets.

(6) The Regulatory Authority shall stipulate the period for which benchmarks will remain unchanged, the historic reference periods against which compliance with benchmarks will be examined and the conditions under which the content of baskets may be changed or price differentiation within a basket made.

Section 35

Procedures for Approval

(1) Besides the cost information submitted to it, the Regulatory Authority may, in addition,

1. refer, for the purpose of comparison, to the prices of such undertakings as offer like services in comparable competitive markets; any special features of the reference markets are to be taken into account in doing so; and

2. apply, for the purpose of costing efficient service provision, cost accounting methods independent of those used by the undertaking, and refer to cost models in doing so.

Where the cost information submitted to the Regulatory Authority is not sufficient for an examination of the rates requiring approval as referred to in section 32 para 1 in conjunction with

section 33, the Regulatory Authority's decision may be based on an examination according to sentence 1 paras 1 or 2.

(2) In the case of approval as referred to in section 32 para 1 the Regulatory Authority shall examine compliance with the requirements of sections 28 and 31 for each rate separately. In the case of approval as referred to in section 32 para 2 the requirements of section 28 and, for the particular basket, of section 31 are deemed satisfied given compliance with the prescribed benchmarks.

(3) Approval is to be granted wholly or in part when the rates meet the requirements of sections 28 and 31 in accordance with subsection (2) and there are no grounds for denial as set out in sentences 2 and 3. Approval is to be denied when the rates are inconsistent with this Act, in particular with section 28, or with other legal provisions. The Regulatory Authority may also deny approval when the undertaking has failed to submit in full the documentation specified in section 33.

(4) The Regulatory Authority should approve rates for a limited period.

(5) Any approvals wholly or partially approving rates already contractually agreed shall have retroactive effect from the time the SMP undertaking first provided service. In proceedings under section 123 of the Code of Administrative Court Procedure, the court may order payment for the time being of higher rates in respect of which rate proposals have been submitted when it is probable, for the most part, that there is a right to the higher rates being approved; the grounds for such order need not be stated. Where the court requires the Regulatory Authority to approve higher rates, such approval has the retroactive effect referred to in sentence 1 only when an order as referred to in sentence 2 has been issued.

(6) The Regulatory Authority shall publish all approved rates.

Section 36

Publication

(1) The Regulatory Authority shall publish decisions it intends to take on the grouping of services and on specification of the benchmarks according to section 32 para 2 and section 34. Prior to publication it shall give the undertaking to whom the decision is addressed the opportunity to make representations.

(2) In respect of submissions for approval as provided for by section 32 para 1 and in the event of proceeding as provided for by section 31(6) sentences 1 and 2 the Regulatory Authority shall publish all rates measures submitted and planned.

Section 37

Divergence from Approved Rates

(1) An SMP public telecommunications network operator may not charge any rates other than those approved by the Regulatory Authority.

(2) Contracts for services containing rates other than those approved shall become effective subject to the proviso that the approved rates apply in place of the agreed rates.

(3) A contractual or legal obligation to provide service shall continue to apply irrespective of whether or not the rates have been approved. The Regulatory Authority may prohibit advertising for, the conclusion, the preparation or the development of a legal transaction applying rates other than those approved or applying rates not approved but subject to approval.

Section 38

Ex Post Rates Regulation

(1) Rates subject to ex post regulation shall be submitted to the Regulatory Authority two months prior to their planned effective date. Where planned rates would clearly not be compatible with section 28 the Regulatory Authority shall, within a period of two weeks of receiving notice of the measure, prohibit introduction of the rates until such time as it has completed its examination. The Regulatory Authority is to be informed, immediately after conclusion of the contract, of any rates measures for individually agreed services not easily applicable to a number of other users.

(2) Where the Regulatory Authority becomes aware of facts warranting the assumption that rates for access services provided or facilities made available by SMP undertakings are not in compliance with the requirements of section 28, the Regulatory Authority shall open an investigation of the rates without undue delay. It shall inform the undertaking concerned, in writing, that an investigation has been opened. Should the Regulatory Authority not be able to investigate on the basis of the comparable markets principle set out in section 35(1) para 1, it may also proceed as set out in section 33.

(3) The Regulatory Authority shall take a decision within a period of two months of the investigation being opened.

(4) Where the Regulatory Authority establishes that rates do not meet the requirements of section 28, it shall forbid such conduct as is prohibited under this Act and declare the rates objected to invalid as from such time non-compliance was established. At the same time, the Regulatory Authority may order the application of rates which meet the requirements of section 28. Where the SMP provider subsequently submits his own rates proposals the Regulatory Authority shall examine, within a period of one month, whether these rates rectify the breaches of the requirements of section 28 which have been established. Section 37 applies accordingly. Where the Regulatory Authority has established abuse of an SMP position within the meaning of section 28(2) para 3 it shall also issue an order stating how the SMP undertaking has to effect unbundling.

Subchapter 3

Regulation of Rates for Retail Services

Section 39

Rates Regulation for Retail Services

(1) Where facts warrant the assumption that obligations imposed in connection with access issues or with carrier selection and carrier preselection according to section 40 would not result in achievement of the regulatory aims according to section 2(2), the Regulatory Authority may make the rates SMP undertakings charge for retail telecommunications services subject to

approval. The Regulatory Authority should limit the approval requirement to those markets in which sustainable competition is not expected to develop in the foreseeable future. In the event of an approval requirement, sections 31 to 37 apply accordingly. Rates for retail services may not under section 32 para 2 be placed in a basket with rates for access services.

(2) Services according to section 78(2) paras 3 and 4 are subject to ex post regulation; section 38(2) to (4) apply accordingly.

(3) Rates for retail services supplied by SMP telecommunications service providers which are not subject to approval shall be subject to ex post regulation; section 38(2) to (4) apply accordingly. In addition, the Regulatory Authority may, having regard to subsection (1) sentence 1, require SMP undertakings to inform it of rates measures two months prior to their planned effective date. Where planned rates would clearly not be compatible with section 28 the Regulatory Authority shall, within a period of two weeks of notice of the measure, prohibit introduction of the rates until such time as it has completed its examination. The Regulatory Authority is to be informed, immediately after conclusion of the contract, of any rates measures for individually agreed services not easily applicable to a number of other users.

(4) Any undertaking having significant market power in a retail market and obliged to grant access to a service and/or facility according to section 21 which includes components that are likewise essential to a service offer in the retail market shall be obliged to submit at the same time as its planned rates measure for the retail service an offer for the wholesale product which meets, in particular, the requirements of section 28. Where the SMP undertaking fails to submit any such wholesale offer, the Regulatory Authority may, without further examination, forbid it from asking the retail price.

Chapter 4

Other Obligations

Section 40

Carrier Selection and Carrier Preselection

(1) The Regulatory Authority shall require undertakings designated as having significant market power in the provision of connection to and use of the public telephone network at fixed locations, in accordance with sentence 4, to enable their subscribers to access the services of all directly interconnected providers of publicly available telecommunications services. This may be done on a call-by-call basis by dialling a carrier selection code, or by means of preselection, with a facility to override any preselected choice on a call-by-call basis by dialling a carrier selection code. It should also be possible for the subscriber to preselect different carriers for local and national calls. In providing the interconnection required to fulfil this obligation it shall be ensured that, in decisions taken under Part 2, incentives for efficient investment in facilities which will secure more competition in the long term are maintained and that efficient use of the existing network is made by handing over calls at a point in the network close to the subscriber. Any charges to end-users for use of the above-mentioned services and facilities are subject to ex post regulation in accordance with section 38(2) to (4).

(2) Obligations according to subsection (1) should be imposed on other SMP undertakings only when the regulatory aims set out in section 2(2) would not otherwise be achieved. Provided there is sustainable services competition in the retail mobile market, the obligations according to subsection (1) should not be imposed for the mobile market. Sustainable services competition in

the retail mobile market is fair competition between services supplied by public mobile network operators and publicly available services supplied by mobile service providers at the retail level; such fair competition presupposes that providers of publicly available mobile services who are independent of public mobile network operators contribute to a sustainable competitive retail mobile market by means of services based also on wholesale products from the public mobile network operators.

Section 41

Set of Leased Lines

(1) The Regulatory Authority shall require undertakings having significant market power in the provision of part or all of the set of leased lines to provide the minimum set of leased lines as identified in the applicable list of standards drawn up by the Commission on the basis of Article 17 of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108 page 33).

(2) Such undertakings have to publish conditions 3.1. to 3.3. as set out in Annex VII to Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108 page 51). If necessary, the Regulatory Authority may set targets in respect of the supply conditions referred to in condition 3.3.

(3) Sections 27 to 39 apply with regard to rates regulation. The provisions on access regulation laid down in sections 16 to 26 remain unaffected.

Chapter 5

Special Control of Anti-Competitive Practices

Section 42

Anti-Competitive Conduct by an SMP Undertaking

(1) No SMP provider of telecommunications services, of services according to section 78(2) paras 3 and 4 or of telecommunications-based services and no SMP public telecommunications network operator may abuse his position. Abuse is constituted, in particular, by conduct consisting in, directly or indirectly, unreasonably obstructing other undertakings or materially affecting their competitive opportunities without objectively justifiable reason.

(2) Abuse within the meaning of subsection (1) is presumed where an SMP undertaking gives itself, its subsidiaries or partners access to services or facilities it uses internally or offers in the marketplace on more favourable conditions or of a better quality than it applies to other undertakings using the service or facility to provide their own telecommunications or related services, unless the undertaking provides evidence of facts objectively justifying the grant of less favourable conditions.

(3) Abuse within the meaning of subsection (1) is also presumed where an SMP public telecommunications network operator fails to comply with an obligation imposed on him under section 22(1) by delaying the processing of access applications without objective reason.

(4) The Regulatory Authority shall take a decision to end the abuse of significant market power upon application or on its own initiative. For this purpose it may, in relation to an undertaking abusing its position of significant market power, impose or prohibit certain practices and declare agreements wholly or partially invalid. Such decision shall generally be taken within a time limit of four months from the commencement of proceedings. Where an application as referred to in sentence 1 is made, the time limit begins running when the application is received. An application as referred to in sentence 1 may be made by any telecommunications service provider who can assert that his rights have been prejudiced.

Section 43

Surrender of Gain to the Regulatory Authority

(1) Where an undertaking has infringed a Regulatory Authority order according to section 42(4) or intentionally or negligently infringed a provision of this Act and thereby obtained economic gain, the Regulatory Authority should order surrender of the economic gain and impose on the undertaking payment of a corresponding sum of money.

(2) Subsection (1) does not apply where such economic gain has been cancelled out by payment of damages or by the imposition or order of forfeiture. Any undertaking paying damages as referred to in sentence 1 only after the surrender of gain is to be reimbursed with the sum of money up to the level of payments proven.

(3) Where enforcing surrender of gain would result in undue hardship, the order should be limited to a reasonable sum of money or be waived entirely. It should also be waived if the economic gain is insignificant.

(4) The level of economic gain may be estimated. The sum of money to be transferred is to be stated in figures.

(5) Surrender of gain may be ordered only within a period of five years of cessation of the infringement and for a maximum period of five years.

PART 3

CUSTOMER PROTECTION

Section 44

Right to Damages and Injunctive Relief

(1) Any undertaking infringing this Act, an ordinance having the force of law issued under this Act, an obligation imposed under this Act in an assignment, or an administrative order of the Regulatory Authority shall be obliged, in relation to the person affected, to eliminate the harmful practice and, where there is danger of further harmful practices, to cease and desist. Such right exists as soon as there is danger of an offence. A person affected is any consumer or competitor harmed by the infringement. Any undertaking to which intent or negligence can be imputed shall also be liable, in relation to a consumer or competitor, to reparation of any damage caused by the infringement. The undertaking has to pay interest on financial debts according to sentence 4 from such time as the damage occurred. Sections 288 and 289 sentence 1 of the Civil Code apply accordingly.

(2) Any person infringing, in a manner other than by using or recommending general terms and conditions, provisions of this Act or provisions of an ordinance having the force of law issued under this Act whose purpose is to protect the consumer, may, in the interest of consumer protection, be required to cease and desist by the bodies named in section 3 of the Injunctions Act. Where offences in a business are committed by an employee or an agent, the right to injunctive relief also applies in relation to the owner of the business. The Injunctions Act remains unaffected in all other respects.

Section 45

Customer Protection Ordinance

(1) The Federal Government shall be empowered, for the special protection of end-users (customers), consumers in particular, to issue, by ordinance having the force of law and requiring the consent of the German Bundestag and the German Bundesrat, framework provisions for using telecommunications services and for ensuring metering and billing accuracy. Particular account is to be taken in doing so of the interests of persons with disabilities. The ordinance shall detail the powers of the Regulatory Authority. Account is to be taken most notably of Articles 21 and 22 of Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108 page 51).

(2) The ordinance may, in particular, make arrangements about the conclusion, the subject matter and the termination of contracts and the rights and obligations of the contracting parties and of the other parties engaged in telecommunications traffic, including the information requirements according to Annex II to Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108 page 51). The ordinance may also stipulate that particular measurement methods be applied in relation to quality of service and that undertakings' general terms and conditions include details of delivery periods and quality of service.

(3) Detailed arrangements, in particular, are to be made in the ordinance with regard to

1. the liability of undertakings;

2. the way in which reference is made to general terms and conditions and to rates and the possibility of their inclusion;

3. information requirements and regulations applicable in the event of non-compliance with these requirements;

4. requirements deriving from Annex I Part A to Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108 page 51) to be met by undertakings in order that their customers can monitor and control their expenditure;

5. entries in directories and directory enquiry service databases;

6. out-of-court dispute resolution procedures for customers; and

7. declarations from property owners.

Section 46

Number Portability, European Telephone Numbering Space

(1) Public telephone network operators shall make provision in their networks to enable subscribers to retain their telephone number, independently of the undertaking providing the telephone service, as follows–

1. in the case of geographic numbers, at a specific location; and

2. in the case of non-geographic numbers, at any location.

The arrangement in sentence 1 applies only within the numbering ranges and subranges designated for a telephone service. In particular, the porting of telephone numbers for telephone services provided at a fixed location to those not provided at a fixed location and vice versa is not permitted.

(2) Providers of publicly available telecommunications services shall ensure that their end-users can retain in conformity with subsection (1) telephone numbers allocated to them when changing to another provider of publicly available telecommunications services.

(3) Subscribers may be charged solely the one-time costs incurred for changing provider. The same applies to costs charged by a network operator to a provider of publicly available telecommunications services. All such rates are subject to ex post regulation as provided for by section 38(2) to (4).

(4) Public telephone network operators have to make provision in their networks for handling all calls to the European telephone numbering space.

Section 47

Provision of Subscriber Data

(1) Every undertaking providing publicly available telecommunications services and assigning telephone numbers to end-users shall be obliged, in observance of the requirements of the relevant data protection legislation, to provide, upon request, any other undertaking with subscriber data as referred to in subsection (2) sentence 4 for the purpose of providing publicly available directory enquiry services and directories. Such data has to be provided without undue delay and in non-discriminatory manner.

(2) Subscriber data are such data as are published in directories of subscribers in accordance with section 104. Besides the number this includes the actual data for publication, ie the subscriber's name and address and any additional information known to the undertaking such as occupation, branch, type of line and co-users. It also includes such information, links, assignments and classifications, processed and presented in line with the state of the art, in observance of the requirements of the relevant data protection legislation and in appropriate form for the customer's use, as are required for the publication of such data in publicly available directory enquiry services and directories according to sentence 1. The data shall be complete and their content and technical form processed and presented in such manner as to allow, under

the state of the art, easy inclusion in a customer-friendly directory or corresponding directory enquiry service database.

(3) In the event of disputes arising between undertakings concerning rights and obligations under subsections (1) and (2), section 133 applies accordingly.

(4) For the provision of subscriber data charges may be levied; such charges will typically be subject to ex post regulation as provided for by section 38(2) to (4). Such charges should be subject to approval under section 31 only when the undertaking has significant market power in the market for retail services.

PART 4

BROADCASTING

Section 48

Interoperability of Television Sets

(1) Every analogue television set with an integral viewing screen of visible diagonal greater than 42 centimetres offered for sale, rent or otherwise made available shall be fitted with at least one interface socket standardised by a recognised European standardisation body, permitting the connection of digital television receivers.

(2) Every digital television receiver offered for sale, rent or otherwise made available shall,

1. if it has an integral viewing screen of visible diagonal greater than 30 centimetres, be fitted with at least one interface socket, standardised by a recognised European standardisation body or conforming to a common, industry-wide, open specification, permitting the connection of digital television receivers and the possibility of conditional access;

2. if it is fitted with an application programming interface, fulfil the minimum requirements of such interface as adopted by a recognised European standardisation body or conforming to a common, industry-wide, open interface specification, enabling third parties to produce and operate their own applications irrespective of the transmission mode.

(3) Every digital television receiver offered for sale, rent or otherwise made available and intended for conditional access shall be capable of displaying signals

1. conforming to the common European scrambling algorithm as administered by a recognised European standardisation body;

2. that do not require conditional access. With regard to rented equipment this applies only inasfar as the rentee is in compliance with the relevant rental agreement.

Section 49

Interoperability of Digital Television Signal Transmissions

(1) Public telecommunications network operators transmitting digital television signals shall retransmit all such signals as are transmitted for representation wholly or partially in the 16:9 screen format, in this format.

(2) Rights holders of application programming interfaces are obliged to provide, on fair, reasonable and non-discriminatory terms and against appropriate remuneration, manufacturers of digital television receivers and third parties claiming a legitimate interest with all such information as is necessary to provide all the services supported by the application programming interface in fully functional form. The criteria referred to in sections 28 and 42 apply.

(3) In the event of a dispute arising between the parties concerned with regard to compliance with the provisions of subsections (1) to (2), either of the parties concerned may refer the matter to the Regulatory Authority. The Regulatory Authority shall take a decision, after hearing the parties concerned, within a period of two months. In proceeding, the Regulatory Authority shall give the authority responsible under state law the opportunity to comment. Where the authority responsible under state law raises objections to do with media legislation, it shall take a decision on the matter within the specified period. The two decisions may be taken in combined proceedings.

(4) Parties concerned shall comply with an order issued by the Regulatory Authority under subsection (3) without undue delay, except where the Regulatory Authority has stipulated a different period. To enforce such order, the Regulatory Authority may set a penalty not exceeding 500,000 euros in accordance with the Administrative Enforcement Act.

Section 50

Conditional Access Systems

(1) Providers of conditional access systems shall ensure that these have the necessary technical capability for the cost-effective transfer of control functions, allowing the possibility for full control by public telecommunications network operators at local or regional level of the services using such conditional access systems.

(2) Holders of industrial property rights to conditional access systems deciding to grant licences to manufacturers of digital television receivers or to third parties demonstrating a legitimate interest shall do so on fair, reasonable and non-discriminatory terms. The criteria referred to in sections 28 and 42 apply. Holders of such rights may take reasonable account of technical and commercial factors. However, licence grant may not be made subject to conditions hindering the installation of

1. a common interface allowing connection with other conditional access systems; or

2. components specific to another conditional access system, for reasons of transaction security with regard to the content to be protected.

(3) Providers and users of conditional access systems shall

1. enable all broadcasters to use the technical services they need to use their systems and to obtain the information they require on fair, reasonable and non-discriminatory terms;

2. where they are also responsible for billing end-users, give the end-user a tariff schedule prior to concluding with him a contract under which charges will be incurred;

3. keep separate accounts for their business as conditional access system providers;

4. prior to beginning to provide service and to providing service with differences, notify the Regulatory Authority of the details referred to in paras 1 to 3, the individual services offered to end-users and the rates charged.

(4) The Regulatory Authority shall inform, without undue delay, the authority responsible under state law of notifications according to subsection (3) para 4. Where the Regulatory Authority or the authority responsible under state law, each for its own area of responsibility, concludes on the basis of the notification within a period of two months that the service offer fails to comply with the requirements specified in subsection (3) paras 1 to 4, they shall require the service offer to be modified. Where the requirements cannot be satisfied despite the modifications or where the modifications have not been made despite the request, they shall prohibit the service offer.

(5) Where one or more providers or users of conditional access systems do not have significant market power, the Regulatory Authority may amend or withdraw conditions according to subsections (1) to (3) with respect to the party or parties concerned, provided that

1. the prospects for effective competition in the retail markets for the transmission of broadcasting signals and for conditional access systems and other associated facilities would not be adversely affected by such amendment or withdrawal; and

2. the authority responsible under state law has established that capacity determinations and must-carry obligations set out in state law would not be adversely affected by such amendment or withdrawal.

Sections 11 to 14(1) apply accordingly to the procedure referred to in sentence 1. Decisions as referred to in sentence 1 shall be reviewed by the Regulatory Authority every two years.

Section 51

Dispute Resolution

(1) Persons with entitlements or obligations under the provisions of this Part may jointly refer to the Dispute Resolution Panel for resolution any contentious issues concerning the application of these provisions. Such referral shall be in written form. The Regulatory Authority shall take a decision within a period of two months.

(2) The Dispute Resolution Panel shall be established at the Regulatory Authority. It shall comprise a Chairman and two Assessors. The Regulatory Authority shall be responsible for establishing the Dispute Resolution Panel, appointing its members and adopting its rules of procedure. The establishment and composition of the Dispute Resolution Panel and its rules of procedure are to be published by the Regulatory Authority.

(3) In proceeding, the Dispute Resolution Panel shall give the authority responsible under state law the opportunity to comment. Where the authority responsible under state law raises objections to do with media legislation, it shall take a decision on the matter within the specified period. The two decisions may be taken in combined proceedings.

PART 5

GRANT OF FREQUENCIES, NUMBERS AND RIGHTS OF WAY

Chapter 1

Frequency Regulation

Section 52

Functions

(1) In order to secure efficient and interference-free use of frequencies and in consideration of the further aims set out in section 2(2), a National Table of Frequency Allocations and a Frequency Usage Plan shall be drawn up, frequencies assigned and frequency usages supervised.

(2) The Regulatory Authority shall issue orders with regard to the use of frequencies for the operation of radio equipment in foreign vehicles, watercraft and aircraft operating within the area of application of this Act.

(3) With regard to the use of frequencies within the area of responsibility of the Federal Ministry of Defence, the Federal Ministry of Economics and Labour shall reach agreement with the Federal Ministry of Defence.

Section 53

Frequency Band Allocation

(1) The Federal Government is empowered, by ordinance having the force of law but not requiring the consent of the German Bundesrat, to stipulate frequency band allocation for the Federal Republic of Germany in a National Table of Frequency Allocations and to amend such Table. Ordinances in which frequencies are allocated to broadcasting require the consent of the German Bundesrat. To be included in their preparation shall be all persons likely to be affected by the allocations.

(2) The National Table of Frequency Allocations allocates frequency bands to radio services and other applications of electromagnetic waves. Insofar as is necessary to secure efficient and interference-free use of frequencies, the Table also includes provisions on the use of frequencies and associated detailed determinations. Sentence 2 also applies to the use of frequencies in and along conductors; for the frequency bands concerned, geographic, time-related and technical determinations are to be made, compliance with which allows free use.

Section 54

Frequency Usage Plan

(1) The Regulatory Authority shall draw up the Frequency Usage Plan on the basis of the National Table of Frequency Allocations in consideration of the aims set out in section 2(2), European harmonisation, technological advance and the compatibility of frequency usages in the transmission media.

(2) The Frequency Usage Plan shall include further allocation of the frequency bands to frequency usages, and determinations on such usages. The Frequency Usage Plan may consist of subplans.

(3) The Frequency Usage Plan shall be drawn up with the participation of the public. The Federal Government is empowered to lay down, by ordinance having the force of law and requiring the consent of the German Bundesrat, the procedure for drawing up the Frequency Usage Plan.

Section 55

Frequency Assignment

(1) Each frequency usage requires prior frequency assignment, unless otherwise provided for by this Act. Frequency assignment means authorisation given by a public authority or by legal provisions to use particular frequencies under specified conditions. Frequencies are assigned for a particular purpose in accordance with the Frequency Usage Plan and in non-discriminatory manner on the basis of transparent and objective procedures. Assignment is not required where usage rights may be exercised by virtue of another statutory regulation. Where it is necessary for public authorities, in order to exercise legal powers, to use frequencies already assigned to other persons and significant interference to these usages is not anticipated as a result of doing so, this usage shall be permitted, subject to the framework conditions established in consultation with the law enforcement agencies, without an assignment being required.

(2) Frequencies are typically assigned ex officio by the Regulatory Authority as general assignments for the use of particular frequencies by the general public or a group of persons defined or capable of being defined by general characteristics. Such assignments are published.

(3) Where general assignment is not possible, frequencies for particular usages are assigned by the Regulatory Authority to natural persons, legal entities and associations of persons, insofar as they may be eligible, upon written application, as individual assignments. This applies in particular when the risk of harmful interference cannot otherwise be ruled out or when this is necessary in order to secure efficient use of frequencies.

(4) The application referred to in subsection (3) has to specify the area in which the frequencies are to be used. The applicant has to show that the subjective requirements for frequency assignment with regard to efficient and interference-free use of frequencies and other conditions as specified in Part B of the Annex to Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) (OJ L 108 page 21) are satisfied. The Regulatory Authority shall take a decision on complete applications within a period of six weeks. This time limit shall not affect existing international agreements on the use of radio frequencies and orbit positions.

(5) Frequencies shall be assigned subject to

1. their designation for the planned usage in the Frequency Usage Plan;
2. their availability;
3. their compatibility with other frequency usages; and

4. their efficient and interference-free use by the applicant being secured.

Applicants are not entitled to any one particular frequency.

(6) The Regulatory Authority is to be notified without undue delay of the beginning and the cessation of usage. It shall also be notified of any change of name, change of address, change in ownership structure and any identity-preserving transformations.

(7) Applications for a change in the frequency assignment are to be submitted without undue delay to the Regulatory Authority, in writing, with supporting documents, when

1. frequency usage rights are to be transferred by singular or universal succession;

2. frequencies are to be transferred to an affiliated undertaking as defined in section 15 of the Stock Corporation Act;

3. frequencies are to be transferred from a natural person to a legal entity in which the natural person holds a share; or

4. an heir intends to continue using the frequencies.

In these cases, the frequencies may continue to be used until such time as a decision is taken on the application for a change in the assignment. The application shall be granted when the requirements for frequency assignment according to subsection (4) are satisfied, distortion of competition in the relevant product and geographic market is not to be feared and the efficient and interference-free use of frequencies is secured. Any frequencies no longer used are to be returned without undue delay by means of a written declaration. Where a legal entity that has been assigned frequencies is liquidated without there being a legal successor, the frequencies shall be returned by the liquidator. Where a natural person dies without an heir intending to continue using the frequencies, these shall be returned by the heir or by the estate administrator.

(8) Frequencies are typically assigned for a limited period, with the possibility of extension. The time limit shall be appropriate to the service concerned.

(9) Where frequencies are not available for assignment in sufficient numbers or where more than one application has been made for particular frequencies the Regulatory Authority may order, without prejudice to subsection (5), that assignment be preceded by award proceedings based on conditions according to section 61 as determined by the Regulatory Authority. Persons likely to be affected are to be heard prior to such decision. The Regulatory Authority's decision is to be published.

(10) A frequency assignment may be denied in full or in part where the use intended by the applicant is incompatible with the regulatory aims according to section 2(2). Where the interests of the federal states relating to broadcasting within their jurisdiction are concerned, consultation is to be held with the state authority with competence, based on the broadcasting regulations.

Section 56

Orbit Positions and Frequency Usage by Satellites

(1) All exercise of German rights to orbit and frequency usage shall require, in addition to frequency assignment according to section 55(1), assignment of such rights by the Regulatory Authority. The Regulatory Authority shall, upon application, perform the advance publication, coordination and notification of satellite systems with the International Telecommunication Union and assign to the applicant the resulting rights to orbit and frequency usage. The preconditions for this are as follows–

1. the availability of frequencies and orbit positions;

2. compatibility with other frequency usages and other satellite system notifications;

3. no detriment to public interest.

(2) With regard to existing German entries in the Plan and other unused rights to orbit and frequency usage with the International Telecommunication Union, award proceedings may be conducted based on conditions as determined by the Regulatory Authority.

(3) Assignment may be revoked where such rights have not been exercised for more than one year or where the preconditions of subsection (1) sentence 3 are no longer given.

Section 57

Special Preconditions for Frequency Assignment

(1) The assignment of frequencies for broadcasting within the jurisdiction of the federal states requires, in addition to the preconditions of section 55, consultation with the state authority with competence, based on the broadcasting regulations. The relevant state authority notifies the Regulatory Authority of the coverage requirements for broadcasting within the jurisdiction of the federal states. The Regulatory Authority shall satisfy these notified requirements in assigning frequencies under section 55. Details of the procedure shall be laid down by the Regulatory Authority on the basis of the broadcasting regulations of the state authorities with competence. Frequencies allocated to the broadcasting service in the National Table of Frequency Allocations and designated in the Frequency Usage Plan may be used for purposes other than broadcasting within the jurisdiction of the federal states where the capacity allocated to broadcasting on the basis of the broadcasting regulations is available. For this purpose the Regulatory Authority shall bring about consultation with the state authorities with competence.

(2) Frequency usages of the Federal Ministry of Defence in the bands designated in the Frequency Usage Plan exclusively for military purposes shall not require assignment.

(3) Frequencies designated in the Frequency Usage Plan for maritime shipping, inland waterways shipping and the aeronautical service and used for such purposes on foreign watercraft or aircraft operating within the area of application of this Act shall be deemed assigned.

(4) With regard to frequencies designated in the Frequency Usage Plan for public safety radiocommunications, the Federal Ministry of the Interior shall, in consultation with the supreme state authorities responsible, determine in a directive the following matters–

1. the responsibilities of the authorities concerned;

2. the procedure for being recognised as qualified to participate in public safety radiocommunications;

3. the procedure for processing applications for the assignment of frequencies for public safety radiocommunications purposes and the responsibilities in this regard;

4. the principles of frequency planning and the procedures for frequency coordination for public safety radiocommunications purposes; and

5. the arrangements for radio operations for and cooperation between and among the authorities and organisations using frequencies for public safety radiocommunications purposes.

The directive is to be drawn up in agreement with the Regulatory Authority, in particular as far as paras 4 and 5 are concerned. The Federal Ministry of the Interior shall confirm in each instance, after hearing the supreme federal or state authorities responsible for the matter, that an applicant is one of the group recognised as qualified according to sentence 1.

(5) Frequencies for use by aeronautical stations in the aeronautical mobile service and aeronautical radionavigation land stations shall be assigned only when consent to install and operate such stations as required by section 81(1) and (2) of the Air Traffic Licensing Ordinance has been given.

(6) Frequencies for use by coast stations in the port operations service shall be assigned only when the consent of the waterways and shipping administration is to hand.

Section 58

Variant Frequency Usages

In justified particular cases, notably to test innovative technologies in telecommunications or to provide frequencies required at short notice, frequency assignments which are at variance with the determinations of the National Table of Frequency Allocations or the Frequency Usage Plan may be granted on a temporary basis, on condition that no degradation is caused to any frequency usage entered in the National Table of Frequency Allocations or the Frequency Usage Plan. No such variance may interfere with the further development of the Tables or Plans. Where the interests of the federal states relating to broadcasting within their jurisdiction are concerned, consultation is to be held with the state authority with competence, based on the broadcasting regulations.

Section 59

Shared Use

Frequencies whose use by one party alone is not expected to be efficient may be assigned to more than one party for shared use. Such assignees shall tolerate any degradation arising from shared use of the frequency for the intended purpose.

Section 60

Constituent Parts of Frequency Assignment

(1) The frequency assignment is to specify, in particular, the type and extent of the frequency usage, insofar as is necessary to secure efficient and interference-free use of frequencies. Use of assigned frequencies may be made solely with radio equipment intended or marked for operation in the Federal Republic of Germany.

(2) In order to secure efficient and interference-free use of frequencies, secondary conditions may be attached to the frequency assignment. Where, after assignment, it is established that usage is being significantly restricted on account of increased use of the radio spectrum or that considerable efficiency gains are possible on account of technological advance, the type and extent of the frequency usage referred to in subsection (1) may be subsequently modified. Where the interests of the federal states relating to broadcasting within their jurisdiction are concerned, consultation is to be held with the state authority with competence, based on the broadcasting regulations.

(3) The frequency assignment should contain references to the parameters for the receiving equipment on which the Regulatory Authority has based its specifications on the type and extent of the frequency usage. The Regulatory Authority takes no measures of any kind to counteract detrimental effects resulting from non-compliance with the parameters notified.

(4) Frequencies for broadcasting within the jurisdiction of the federal states shall be assigned, in consultation with the state authority with competence, subject to conditions ensuring that the broadcasting interests of the federal states are taken into account.

Section 61

Award Proceedings

(1) Where an order has been issued under section 55(9) requiring frequency assignment to be preceded by award proceedings, the Regulatory Authority may, after hearing the parties concerned, conduct an auction in accordance with subsection (5) or invite tenders in accordance with subsection (6). Decisions on the choice of proceedings and the determinations and rules for the conduct of proceedings are to be published by the Regulatory Authority. Frequency assignment shall be effected in accordance with section 55 following completion of the award proceedings referred to in sentence 1.

(2) As a general rule, the proceedings laid down in subsection (5) are to be conducted, except where such proceedings are not likely to secure the regulatory aims according to section 2(2). This may be the case, in particular, when frequencies have already been assigned, without a prior auction, in the relevant product and geographic market for which the radio frequencies may be used in observance of the Frequency Usage Plan, or where an applicant can claim a legal right to preference for the frequencies to be assigned. The proceedings laid down in subsection (5) are not applicable in respect of frequencies intended for broadcasting services.

(3) An applicant may be excluded from participation in award proceedings where a successful bid according to subsection (5) by him or a successful tender according to subsection (6) from him is expected to prejudice fair competition in the relevant product and geographic market for which the radio frequencies to be assigned may be used in observance of

the Frequency Usage Plan. Any such decision shall take due account of the legitimate interests of the particular applicant in the deployment of new technologies.

(4) The aim of award proceedings is to determine which of the applicants is or are best placed to make efficient use of the frequencies to be assigned. Prior to carrying out award proceedings, the Regulatory Authority shall determine the following matters–

1. the minimum specialist and other requirements to be met by applicants in order to qualify for the award proceedings;

2. the relevant product and geographic market for which the frequencies to be assigned may be used in observance of the Frequency Usage Plan;

3. the basic spectrum package required for commencement of the telecommunications service, where necessary;

4. the frequency usage conditions, including the degree of coverage with the frequency usage and the time required to achieve such degree.

(5) In the case of an auction, the Regulatory Authority shall, prior to the award proceedings, detail the rules for conducting auctions; such rules shall be objective, transparent and non-discriminatory and have regard to the interests of small and medium-sized enterprises. The Regulatory Authority may stipulate a minimum bid for participation in the auction.

(6) In the case of tendering, the Regulatory Authority shall, prior to the award proceedings, determine the criteria against which tenderers' eligibility will be assessed. Such criteria are the tenderers' specialist knowledge and efficiency, the suitability of their plans for providing the telecommunications service for which the tender has been invited, and the promotion of sustainable competition in the market. Preference is to be given in the selection procedure to tenderers ensuring a higher degree of coverage with the particular telecommunications services. The Regulatory Authority shall also detail the rules for tendering; such rules shall be objective, transparent and non-discriminatory. Where the outcome of tendering shows several tenderers to be equally well placed, the decision shall be made by drawing lots.

(7) Any commitments entered into by bidders in the course of an auction or by tenderers in the course of tendering shall become constituent parts of the frequency assignment.

(8) In the case of an auction according to subsection (5) or tendering according to subsection (6), the maximum period of six weeks referred to in section 55(4) may be extended by as long as necessary, but by no more than eight months, however, in order to ensure a fair, reasonable, open, and transparent procedure for all concerned. Such time limits shall be without prejudice to existing international agreements on spectrum use and satellite coordination.

Section 62

Spectrum Trading

(1) The Regulatory Authority may, after hearing the parties concerned, release frequency bands for trading and stipulate the framework conditions of and the procedure for trading when there is interest in trading usage rights for the spectrum concerned. The procedure shall include termination of the frequency assignment and the issue of a new assignment.

(2) The framework conditions of and the procedure for trading shall ensure, in particular, that

1. spectrum efficiency is increased or maintained;

2. the original award proceedings do not preclude frequency assignment after spectrum trading;

3. no distortion of competition in the relevant product and geographic market is to be feared;

4. other legal framework conditions, in particular the conditions of use and international agreements on spectrum use, are complied with; and

5. the regulatory aims according to section 2(2) are secured.

Decisions on the framework conditions of and the procedure for spectrum trading are to be published. With regard to frequencies intended for the broadcasting services, decisions shall be taken in agreement with the authority responsible under state law.

(3) Proceeds from spectrum trading, less the administrative costs incurred, are due to the party selling the usage rights.

Section 63

Revocation of Frequency Assignment, Relinquishment

(1) A frequency assignment may be revoked where use of the assigned frequency for the intended purpose has not commenced within one year of the assignment or where the frequency has not been used for the intended purpose for more than one year.

(2) The frequency assignment may also be revoked, apart from in the cases specified in section 49(2) of the Administrative Procedures Act, where

1. one of the preconditions according to section 55(5) and section 57(4) to (6) is no longer given;

2. an obligation arising from the assignment is repeatedly violated or has not been fulfilled despite repeated requests for fulfilment;

3. competition or the introduction of new spectrum-efficient technologies is prevented or unreasonably hindered as a result of a scarcity of frequencies which arises after the assignment; or

4. distortion of competition in the relevant product and geographic market is to be feared as a result of a change in ownership structure in the person of the assignee.

The period of time until revocation becomes effective shall be appropriate. Where frequencies for broadcasting within the jurisdiction of the federal states are concerned, the Regulatory Authority shall consult the state authority with competence, on the basis of the broadcasting regulations.

(3) The frequency assignment should be revoked where, in respect of a frequency assigned for broadcasting within the jurisdiction of the federal states, all the broadcasting regulations from

the state authority with competence concerning transmissions on the given frequency have ceased to apply. In place of the revocation according to sentence 1, the Regulatory Authority may, when, in respect of a frequency according to sentence 1, one or all of the broadcasting regulations according to sentence 1 has or have ceased to apply and no new broadcasting regulation has been issued within a period of six months, assign, in accordance with the Frequency Usage Plan, in consultation with the state authority with competence, such frequency to the previous assignee – possibly even in derogation of the previous award proceedings – with a limited obligation or with no obligation to use it for broadcasting within the jurisdiction of the federal states.

(4) Section 49(6) of the Administrative Procedures Act is not applicable to revocation according to subsections (2) and (3).

(5) The Regulatory Authority should revoke frequency assignments for analogue broadcast transmissions on the basis of the broadcasting regulations of the state authority with competence, in accordance with the Frequency Usage Plan, not later than 2010 for television broadcasting and not later than 2015 for VHF sound broadcasting. Sound broadcast transmissions in the low, medium and high frequency bands remain unaffected. The frequency assignment shall expire after an appropriate period of time as specified in the revocation but in no case of less than one year.

(6) The frequency assignment shall expire upon relinquishment. Relinquishment is to be declared to the Regulatory Authority in writing, with the exact designation of the frequency assignment being stated.

Section 64

Monitoring, Orders to Take Equipment Out of Service

(1) The Regulatory Authority shall monitor frequency usage in order to secure the aims of frequency regulation. Insofar as is necessary and reasonable for this purpose, most notably to identify a particular frequency user, Regulatory Authority staff are authorised to obtain information on the detailed circumstances of a telecommunications activity and also, in special cases, to listen in to emissions. Information obtained as a result of the measures referred to in sentence 2 may be used solely for the purpose of securing the aims of frequency regulation. In derogation of this, information may be transmitted to the authorities responsible where this is necessary to prosecute a criminal offence as set out in section 100a of the Code of Criminal Procedure. The basic right of privacy of telecommunications laid down in Article 10 of the Basic Law shall be restricted in accordance with sentences 2 to 4.

(2) The Regulatory Authority may, to secure the aims of frequency regulation, order that equipment be operated with restrictions or be taken out of service. To enforce such administrative orders, a penalty not exceeding 500,000 euros may be set in accordance with the Administrative Enforcement Act.

Section 65

Restrictions on Frequency Assignments

Use of assigned frequencies may be restricted on a temporary basis where such frequencies are required by the authorities responsible to perform their duties in a state of tension or defence, in connection with alliance commitments, in connection with cooperation with the

United Nations, in connection with international emergency management or in the event of a natural disaster or a particularly serious accident.

Chapter 2
Numbering

Section 66
Numbering

(1) The Regulatory Authority shall discharge numbering functions. It shall be responsible, in particular, for structuring and configuring the numbering space with the aim of satisfying the requirements of end-users, telecommunications network operators and telecommunications service providers. The Regulatory Authority shall also allocate numbers to telecommunications network operators, telecommunications service providers and end-users. Not included in its responsibilities is the administration of the country code top level and lower level domains.

(2) In order to implement international obligations and recommendations and to ensure sufficient availability of numbers, the Regulatory Authority may modify the structure and configuration of the numbering space and the national numbering plan. In doing so, it shall take reasonable account of the interests of the parties concerned, most notably of the conversion costs incurred by operators, telecommunications service providers and users. Proposed modifications are to be made known in good time prior to becoming effective. Telecommunications network operators and telecommunications service providers affected by such modifications are required to take all implementation measures necessary.

(3) The Regulatory Authority may issue orders to enforce the obligations referred to in subsection (2). To enforce such orders, a penalty not exceeding 500,000 euros may be set in accordance with the Administrative Enforcement Act.

(4) The Federal Government shall be empowered to lay down, by ordinance having the force of law and requiring the consent of the German Bundestag and the German Bundesrat, the criteria and guidelines for the structuring, configuration and administration of numbering space, for the acquisition, the extent and the loss of rights to use numbers including the requirements for telecommunications-based services, and to transpose international recommendations and obligations into national legislation. In doing so it shall take account, in particular, of an efficient use of numbers, the interests of the market players including their interest in a sound basis for planning, the economic implications for the market participants, the requirements in respect of the use of numbers and of meeting demand in the long term, and the interests of the end-users. The powers of the Regulatory Authority and the rights and obligations of the market participants and of the end-users are to be detailed in the ordinance. Subsection (1) sentence 4 applies accordingly.

Section 67
Powers of the Regulatory Authority

(1) The Regulatory Authority may, under its responsibility for numbering administration, issue orders and take any other suitable measures to secure compliance with the legal provisions and with the conditions it has imposed in connection with the allocation of numbers. In particular, the Regulatory Authority may, where statutory obligations or obligations imposed by public

authorities have not been fulfilled, withdraw the unlawfully used number. Further, where it has reliable information on the unlawful use of a telephone number, it should issue an order in relation to the operator of the network in which the number is activated to deactivate the telephone number. The Regulatory Authority may, where it has reliable information on unlawful use, request the bill-issuer not to issue bills for the number concerned. In justified exceptional cases the Regulatory Authority may prohibit certain categories of dialler; the Regulatory Authority shall lay down details of the procedure governing such prohibition.

(2) The rights of the federal states and the powers of other public authorities are not affected.

(3) The Regulatory Authority shall notify the public prosecutor or the administrative authority of any facts giving reason to suspect a criminal or an administrative offence.

Chapter 3
Rights of Way

Section 68
Principle of the Use of Public Ways

(1) The Federation shall have the power to use trafficways free of charge for telecommunications lines serving public purposes, provided that their dedication as trafficways is not thereby restricted on a lasting basis (right of use). Trafficways shall include public ways, squares, bridges and public waters.

(2) Telecommunications lines are to be installed and maintained in such a way as to satisfy the requirements of public safety and order and to comply with the recognised rules of engineering.

(3) The installation of new and the modification of existing telecommunications lines shall require the written consent of the authorities responsible for the construction and maintenance of public ways. With regard to the installation of overhead lines the interests of the above authorities, of public telecommunications network operators and the requirements of town planning shall be weighed. Where installation can be coordinated under a comprehensive building project to be carried out close in time to the application for consent, lines should typically be installed underground. Consent may be given subject to secondary conditions which are to be framed in non-discriminatory manner; consent may also be made dependent on payment of a reasonable security. Such secondary conditions may make stipulations solely on the way in which a telecommunications line is to be installed, the rules of engineering to be observed in doing so, the safety and ease of traffic, the records, consistent with the local practices of the above authority, on the location of a telecommunications line by geographic coordinates, and traffic safety obligations.

(4) Where the authority responsible for the construction and maintenance of public ways is itself the operator of a telecommunications line or has merged within the meaning of section 37(1) or (2) of the Competition Act with an operator, consent according to subsection (3) is to be given by an administrative body which is independent of the administrative body responsible for operation of the telecommunications line or for the exercise of corporate rights, as the case may be.

Section 69

Transfer of Rights of Way

(1) The Federation shall, upon written application, transfer to public telecommunications network operators its rights of use according to section 68(1) through the Regulatory Authority.

(2) The area for which the right of use is to be transferred is to be named in the application referred to in subsection (1). The Regulatory Authority shall grant the right of use where the applicant has the proven specialist knowledge, reliability and efficiency to install telecommunications lines and the right of use is consistent with the regulatory aims set out in section 2(2). The Regulatory Authority shall grant the right of use for the duration of the public activity. The Regulatory Authority shall decide on complete applications within a period of six weeks.

(3) The beginning and cessation of use and any change of name, change of address or identity-preserving transformations of the undertaking are to be notified without undue delay to the Regulatory Authority. The Regulatory Authority shall provide the authority responsible for the construction and maintenance of public ways with this information. The party enjoying the right of use shall be liable for any damage arising from changes not being notified in time.

Section 70

Shared Use

Insofar as it is not possible, or is possible only at disproportionately high expense, to exercise the right according to section 68 for the installation of further telecommunications lines, acquiescence in the shared use of other installations intended for the accommodation of telecommunications cables can be required where shared use is economically reasonable and no major additional construction work is needed. In this case the party enjoying the right of shared use shall pay adequate compensation in money's worth to the party obliged to grant shared use.

Section 71

Showing Consideration for Maintenance and Dedication

(1) With regard to the use of trafficways, any hindrance to their maintenance and any temporary restriction of their dedication as trafficways is to be avoided as far as possible.

(2) Where maintenance is hindered, the party enjoying the right of use is to reimburse the party liable for maintenance with the costs arising from such hindrance.

(3) After completion of work on the telecommunications lines, the party enjoying the right of use is to restore the trafficway without undue delay, provided the party liable for maintenance has not declared itself willing to undertake restoration itself. The party enjoying the right of use is to reimburse the party liable for maintenance with the expenses incurred for any restoration thus undertaken and to pay compensation for any damage incurred as a result of work on the telecommunications lines.

Section 72

Changes Required

(1) Where, following the installation of a telecommunications line, it emerges that the telecommunications line is restricting a trafficway's dedication as a trafficway more than temporarily or is preventing performance of the work required for its maintenance or is impeding the execution of any modification to the trafficway intended by the party liable for maintenance, the telecommunications line, to the extent necessary, is to be modified or removed.

(2) Where a trafficway is withdrawn, the right of use of the party enjoying such right shall lapse.

(3) In all such cases the party enjoying the right of use is to bring about the required measures in respect of the telecommunications line at its own expense.

Section 73

Protection of Trees

(1) Trees planted on and around trafficways are to be protected where possible and their growth allowed for. Lopping may be required only to the extent necessary to install the telecommunications line or to prevent interruption of service; it is to be limited to the degree that is absolutely necessary.

(2) The party enjoying the right of use is to set the tree owner an appropriate period within which to carry out lopping himself. Where lopping has not been carried out or has not been carried out sufficiently within the specified period, the party enjoying the right of use shall bring about lopping. It shall also be entitled to do so when it is a matter of urgently preventing or eliminating interference.

(3) The party enjoying the right of use shall pay compensation for all damage to trees and repay the costs of all lopping carried out at its request.

Section 74

Special Installations

(1) Telecommunications lines are to be configured in such a way that they do not adversely affect existing special installations (installations serving to maintain public ways, drains, water and gas pipelines, tracks, electrical installations and the like). The party enjoying the right of use is to bear the costs incurred for the implementation of any necessary protective measures.

(2) The relocation or modification of existing special installations may be requested only against compensation and only where the trafficway, otherwise, could not be used for the telecommunications line and the special installation can be placed elsewhere in suitable manner for its intended purpose.

(3) Even if these prerequisites are met, the trafficway shall not be used for the telecommunications line where the damage arising from relocation or modification of the special installation would be disproportionately high in relation to the costs the party enjoying the right of use would incur for use of any other trafficway available to it.

(4) Subsections (1) to (3) apply accordingly with regard to special installations in the preparatory stage whose construction lies in the public interest. Compensation by reason of subsection (2) shall be granted only up to the level of the expenses incurred in the preparations. Installations shall be deemed in a preparatory stage as soon as they have been approved by the client by virtue of the detailed plan of the installation, and, insofar as is necessary, by the competent authorities and by the owner or any other party enjoying the right of use of the way.

Section 75

Subsequent Special Installations

(1) Subsequent special installations are, where possible, to be configured in such a way that they do not adversely affect existing telecommunications lines.

(2) A request to relocate or modify a telecommunications line shall be complied with at the expense of the party enjoying the right of use where a subsequent special installation, the construction of which, for reasons of public interest, in particular for economic or traffic considerations, is to be carried out by the party liable for the maintenance of public ways or with its majority participation, would otherwise not be able to be constructed or the construction of which would be significantly hindered. The relocation of a cable-based telecommunications line not used just for local, suburban or neighbouring area traffic may be required only when such cable-based telecommunications line can be placed elsewhere in suitable manner for its intended purpose without disproportionately high costs being incurred.

(3) Where, as a result of any such subsequent special installation, protective measures on an existing telecommunications line have to be carried out, the costs arising are to be borne by the party enjoying the right of use.

(4) Where a party liable for the maintenance of public ways transfers its share to a third party not liable for maintenance, the party enjoying the right of use is to be reimbursed with the costs incurred for the relocation or modification or for the implementation of protective measures, as far as these concern its share.

(5) Operators of special installations other than those referred to in subsection (2) shall bear the costs incurred for the relocation or modification of existing telecommunications lines or for the implementation of any protective measures required.

(6) With regard to any subsequent modification of existing special installations, subsections (1) to (5) apply accordingly.

Section 76

Detriment to Property

(1) The owner of a property that does not constitute a trafficway within the meaning of section 68(1) sentence 2 cannot prohibit the installation, operation or renewal of telecommunications lines on his property insofar as,

1. on his property, a line or installation that is secured by right is used also for the installation, operation or renewal of a telecommunications line and the usability of the property is not thereby additionally restricted on a lasting basis; or

2. the property is not, or is not significantly, affected by such use.

(2) A property owner having to acquiesce in actions according to subsection (1) may claim appropriate pecuniary compensation from the operator of the telecommunications line or the owner of the network if use of his property or the income from it is affected beyond reasonable measure by the installation, the renewal or by maintenance work, repair work or comparable measures directly connected with the operation of the telecommunications line. In addition, one-time pecuniary compensation for extended use for telecommunications purposes may be claimed, provided there were no lines hitherto that could be used for telecommunications purposes. In the event of damage to the property or its movables from exercise of the rights ensuing from this provision, the operator or the owner of the network shall remove the damage at his expense. Section 840(1) of the Civil Code applies.

Section 77

Damage Claims

The limitation period for claims arising from sections 70 to 76 follows the arrangements on the normal limitation periods set out in the Civil Code.

PART 6

UNIVERSAL SERVICE

Section 78

Universal Services

(1) Universal services are a minimum set of publicly available services of specified quality to which every end-user, irrespective of his place of residence or work, shall have access at an affordable price and whose provision to the public as a basic service has become indispensable.

(2) The following have been determined as universal services–

1. connection at a fixed location to a public telephone network and access to publicly available telephone services at a fixed location including – subject to technical feasibility – the features call waiting, call forwarding and call hold/broker's call;

2. the availability of at least one printed public directory of subscribers (section 104) approved by the Regulatory Authority, which satisfies general requirements and is updated on a regular basis, once a year at least;

3. the availability, to users of public pay telephones as well, of at least one comprehensive public telephone directory enquiry service, including provision of the area codes of domestic subscribers and of subscribers in other countries, as far as the subscriber data are available and in observance of the requirements of the relevant data protection legislation;

4. provision throughout the Federal Republic of Germany, in accordance with general demand, of public pay telephones in general locations accessible to everyone at all times; public pay telephones are to be kept in working order; and

5. the possibility to make emergency calls from all public pay telephones free of charge and without the use of any means of payment by simple use of the number "112" and the national emergency call numbers determined in the ordinance as provided for under section 108(2) sentence 1 para 1.

(3) Undertakings providing the universal services referred to in subsection (2) paras 2 and 3 are to apply the principle of non-discrimination to the treatment of information provided to them by other undertakings.

(4) The Regulatory Authority may, after consulting the undertaking with universal service obligations (designated universal service provider), identify general demand for the universal services referred to in subsection (2) in terms of the needs of end-users with regard to, in particular, geographical coverage, number of telephones, accessibility and quality of service. The Regulatory Authority has the power to impose obligations on undertakings in order to secure provision of the service and of service features. The Regulatory Authority may choose not to impose such obligations for all or part of its territory if it is satisfied, after consulting the interested parties, that these service features or comparable services are deemed widely available.

Section 79

Affordability

(1) The price for the universal service referred to in section 78(2) para 1 is deemed affordable if it does not exceed the real price of the telephone services required on average by a household situated outside a town or city with a population of more than 100,000 on 1 January 1998. The assessment of affordability takes into account the quality of service levels, including supply times, at that time and the rate of growth in productivity up to 31 December of the year prior to the previous one.

(2) The universal services referred to in section 78(2) paras 2 to 4 are deemed affordable if the rates comply with the criteria set out in section 28.

Section 80

Obligation to Provide Universal Service

Where a universal service as referred to in section 78 is not being adequately or appropriately provided by the market or where there is reason to fear that such provision will not be secured, each provider operating in the relevant product market and achieving, within the area of application of this Act, at least four percent of total sales in this market or having significant market power in the relevant geographic market shall be obliged to contribute to making possible provision of the universal service. An obligation as referred to in sentence 1 is to be fulfilled in accordance with the provisions of this Chapter.

Section 81

Imposition of Universal Service Obligations

(1) The Regulatory Authority shall publish its findings of any relevant product and geographic market or of any place in which a universal service as referred to in section 78(2) is not being adequately or appropriately provided or in which there is reason to fear that such provision will

not be secured. It shall announce its intention to proceed as provided for by sections 81 to 87, unless an undertaking declares itself willing, within a period of one month of the publication of notice, to provide such universal service without compensation according to section 82.

(2) The Regulatory Authority may, after consulting the undertakings likely to be concerned, decide whether, and to what extent, to oblige one or more of these undertakings to provide the universal service. Any such obligation may not unduly prejudice the undertakings thus designated in relation to the other undertakings.

(3) Where an undertaking that is to be obliged under subsection (2) to provide a universal service substantiates by prima facie evidence that, in the case of such obligation, it will be able to claim compensation according to section 82, the Regulatory Authority shall, instead of designating one or more undertakings, invite tenders for the universal service and award it to the applicant proving himself well placed to provide, and requiring the least financial compensation for providing, the universal service in compliance with the terms laid down in the provisions of this Act. The Regulatory Authority may, taking into account the criteria of sentence 1, designate different undertakings or groups of undertakings to provide different elements of the universal service or to cover different parts of the federal territory.

(4) Prior to inviting tenders for the universal service, the Regulatory Authority is to determine the criteria against which the eligibility of the universal service provider will be assessed. It is also to detail the rules for inviting tenders; such rules shall be objective, transparent and non-discriminatory.

(5) Where a suitable applicant is not found by tendering, the Regulatory Authority shall oblige the undertaking identified under subsection (2) to provide the universal service in accordance with this Act.

Section 82

Compensation for Universal Service Provision

(1) Where an undertaking is obliged under section 81(3) to provide a universal service, the Regulatory Authority shall grant the financial compensation as recognised in the tendering procedure for the provision of such service.

(2) Where an undertaking is obliged under section 81(5) to provide a universal service, the Regulatory Authority shall determine the compensation payable for such provision by calculating the difference between the cost for a designated undertaking of operating without the universal service obligation and the cost of operating in observance of the obligation. Benefits and proceeds accruing to the universal service provider, including intangible benefits, are also to be taken into account.

(3) The Regulatory Authority shall determine whether the costs identified constitute an unfair burden. In such case the Regulatory Authority shall grant the undertaking, upon application, the financial compensation calculated.

(4) To calculate the amount of compensation, the Regulatory Authority may ask the designated universal service provider for the necessary documentation. The Regulatory Authority is to examine the documentation submitted in particular with a view to the need for service provision. The results of the cost calculation and of the examination are to be published,

the protection of trade and operating secrets of the undertakings concerned being taken into account.

(5) Compensation shall be paid after expiry of the calendar year in which a deficit in providing the universal service was incurred.

Section 83

Universal Service Contributions

(1) Where the Regulatory Authority grants compensation according to section 82 for provision of a universal service, each undertaking obliged under section 80 to provide the universal service shall share, by means of a universal service contribution, in funding the compensation. The sharing mechanism is assessed on the basis of the proportion of the sales of the particular undertaking to the total sales of all those with obligations according to sentence 1 in the relevant product market. Where it is not possible to recover such contribution from an undertaking with liability to pay, the shortfall is to be made up for by the others with obligations on the basis of the proportion of their shares in relation to each other.

(2) After expiry of a calendar year for which compensation according to section 82 subsections (1) or (3) has been granted, the Regulatory Authority shall determine the level of compensation and the shares due from the contributing undertakings and communicate this to the undertakings concerned. The level of compensation is derived from the amount of compensation calculated by the Regulatory Authority plus interest at market rates. Interest is paid as from the day following the date of expiry of the calendar year referred to in sentence 1.

(3) All undertakings contributing in accordance with subsection (1) to compensation are required to pay to the Regulatory Authority the share falling to them as assessed by the Regulatory Authority within a period of one month of receiving the notice of assessment.

(4) Where an undertaking liable to pay compensation is more than three months in arrears with payment of its contribution, the Regulatory Authority shall issue a notice of arrears and enforce collection.

Section 84

Availability, Unbundling and Quality of Universal Services

(1) Where undertakings provide universal services, end-users shall, within the limits of the legislation and general terms and conditions, have a right to the provision of such services.

(2) Undertakings providing universal services are to offer universal services in such a way that the end-user is not obliged to pay for services or facilities which are not necessary or not required for the service requested.

(3) Undertakings providing universal services shall, upon request, supply the Regulatory Authority with and publish adequate and up-to-date information on their performance in the provision of universal service. Such information shall be based on the quality of service parameters, definitions and measurement methods set out in Annex III to Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108 page 51).

Section 85

Suspension of Service

(1) Any undertaking obliged under section 81 to provide universal services or providing services under section 150(9) may suspend or restrict such service only temporarily on account of essential requirements conforming with Community law. It shall have regard to the interests of end-users and limit, as far as technically feasible, such suspension or restriction to the service concerned.

(2) Essential requirements justifying limited universal service are

1. security of network operations;

2. maintenance of network integrity, in particular the prevention of serious interference to the network or damage to software or stored data;

3. interoperability of services; and

4. data protection.

Section 86

Provision of Security

(1) Providers of publicly available telecommunications services obliged under section 81 to provide universal services and the undertaking providing services under section 150(9) shall have the right to make provision of universal services to the end-user conditional upon a reasonable amount of security where there are grounds to believe that the end-user will fail, or will fail within the prescribed period, to honour his contractual obligations. Security may be provided in the form of a surety bond from a financial institution registered in the European Economic Area. The provider shall have the right to limit the provision of security to such surety bond and a money deposit. The security shall be returned or cleared without undue delay as soon as the conditions requiring its provision cease to apply.

(2) Reasonable within the meaning of subsection (1) sentence 1 shall typically be the installation price plus six times the rental price. Any requirement to pay a higher amount shall be justified in relation to the end-user with reference to the circumstances of his particular case.

Section 87

Disclosure of Sales

(1) Where an obligation to provide universal service has been imposed under section 81 subsections (3) or (5), all undertakings operating in the relevant market for the applicable telecommunications services are to inform the Regulatory Authority annually, upon request, of their sales in this market. Otherwise the Regulatory Authority may make an estimate.

(2) With regard to the assessment of sales according to subsection (1), sections 36(2) and 38 of the Competition Act apply accordingly.

(3) The Regulatory Authority shall, taking into account the protection of trade and operating secrets of the undertakings concerned, publish a report annually which sets out the costs, as calculated, of the universal service obligation and the contributions from all the undertakings and which identifies any market benefits that may have accrued to the designated undertaking.

PART 7

PRIVACY OF TELECOMMUNICATIONS, DATA PROTECTION, PUBLIC SAFETY

Chapter 1

Privacy of Telecommunications

Section 88

Privacy of Telecommunications

(1) The content and detailed circumstances of telecommunications, in particular the fact of whether or not a person is or was engaged in a telecommunications activity, shall be subject to telecommunications privacy. Privacy shall also cover the detailed circumstances surrounding unsuccessful call attempts.

(2) Every service provider shall be obliged to maintain telecommunications privacy. The obligation to maintain privacy also applies after the end of the activity through which such commitment arose.

(3) All persons with obligations according to subsection (2) shall be prohibited from procuring, for themselves or for other parties, any information regarding the content or detailed circumstances of telecommunications beyond that which is necessary for the commercial provision of their telecommunications services, including the protection of their technical systems. Knowledge of facts which are subject to telecommunications privacy may be used solely for the purpose referred to in sentence 1. Use of such knowledge for other purposes, in particular, passing it on to other parties, shall be permitted only insofar as provided for by this Act or any other legal provision and reference is made expressly to telecommunications activities. The reporting requirement according to section 138 of the Penal Code shall have priority.

(4) Where the telecommunications system is located on board a ship or an aircraft, the obligation to maintain privacy does not apply in relation to the captain or his second in command.

Section 89

Prohibition to Intercept, Obligation on Receiving Equipment Operators to Maintain Privacy

Interception by means of radio equipment shall be permitted only for communications intended for the radio equipment operator, radio amateurs within the meaning of the Amateur Radio Act of 23 June 1997 (Federal Law Gazette Part I page 1494), the general public or a non-defined group of persons. The content of communications other than those referred to in sentence 1 and the fact of their reception, even where reception has been unintentional, may not, even by persons not already committed to privacy under section 88, be imparted to others.

Section 88(4) applies accordingly. The interception and passing on of communications by special legal authorisation remain unaffected.

Section 90

Misuse of Transmitting Equipment

(1) It shall be prohibited to own, manufacture, market, import or otherwise introduce in the area of application of this Act transmitting equipment which, by its form, purports to be another object or is disguised under an object of daily use and, due to such circumstances, is particularly suitable for intercepting the non-publicly spoken words of another person without his detection or for taking pictures of another person without his detection. The prohibition on owning such transmitting equipment does not apply to any person obtaining or acquiring actual control of transmitting equipment

1. as an executive body, as a member of an executive body, as a legal representative or as a partner entitled to represent a person authorised under subsection (2);

2. from another or for another person authorised under subsection (2) if and for as long as he has to comply by virtue of service or employment relations with the directives given by the other party concerning exercise of the actual control of the transmitting equipment, or exercises actual control by virtue of a court order or an order from a public authority;

3. as a bailiff or an enforcement officer in enforcement proceedings;

4. temporarily, from a person authorised under subsection (2), for the purpose of safe custody or non-commercial conveyance to an authorised person;

5. for conveyance or storage for business purposes only;

6. by finding, provided that such person hands over the equipment without undue delay to the loser, the owner, any other party entitled to acquire the equipment or the office responsible for taking delivery of the lost property report;

7. causa mortis, provided that such person gives the transmitting equipment to an authorised person without undue delay or renders it permanently unusable; or

8. which has been rendered permanently unusable by the removal of a major component, provided that such person gives notice in writing to the Regulatory Authority of the acquisition without undue delay, stating his particulars, the type of equipment, its trademark and any manufacturing number given on the equipment, and presents prima facie evidence that the equipment has been acquired for collection purposes only.

(2) The supreme federal and state authorities with competence shall allow exceptions where these are required in the public interest, in particular for public safety reasons. Subsection (1) sentence 1 does not apply insofar as the Federal Office of Economics and Export Control (BAFA) has authorised export of the transmitting equipment.

(3) It shall be prohibited to advertise, in public or in communications intended for a relatively large group of persons, transmitting equipment by indicating that the equipment is suitable for intercepting the non-publicly spoken words of another person without his detection or for taking pictures of another person without his detection.

Chapter 2
Data Protection

Section 91
Scope

(1) This Chapter regulates the protection of the personal data of telecommunications subscribers and users in respect of the collection and use of such data by undertakings and persons providing telecommunications services on a commercial basis or contributing to such provision. Details, subject to telecommunications privacy, of the circumstances of an identified or identifiable legal person or partnership, to the extent that it is capable of acquiring rights and undertaking commitments, shall have the same status as personal data.

(2) In respect of closed user groups at public authorities of the federal states, this Chapter applies subject to the proviso that the relevant state data protection legislation applies in place of the Federal Data Protection Act.

Section 92
Transfer of Personal Data to Foreign Private Bodies

Service providers shall transfer to foreign private bodies personal data as provided for by the Federal Data Protection Act solely to the extent required for the provision of telecommunications services, for the preparation or dispatch of bills and to combat fraud.

Section 93
Duty to Provide Information

When concluding contracts, service providers shall inform their subscribers of the nature, extent, place and purpose of the collection and use of personal data in such a way that the subscribers are given notice, in readily comprehensible form, of the basic data processing facts. The attention of subscribers shall also be drawn to the choices and options permitted. Users shall be informed by the service provider by means of generally available information about the collection and use of personal data. The right to provision of information as set out in the Federal Data Protection Act remains unaffected.

Section 94
Consent by Electronic Means

Consent may also be given electronically where the service provider ensures that

1. the subscriber or user has given his consent deliberately and unequivocally;
2. consent is recorded;
3. the subscriber or user can access his declaration of consent at any time; and

4. the subscriber or user can withdraw his consent at any time with effect for the future.

Section 95

Contractual Relations

(1) The service provider may collect and use customer data to the extent required to achieve the purpose referred to in section 3 para 3. Under a contractual relationship with another service provider, the service provider may collect and use the customer data of his subscribers and of the subscribers of the other service provider to the extent required for performance of the contract between the service providers. Transmission of the customer data to third parties, unless permitted by this Part or by another law, shall be carried out only with the subscriber's consent.

(2) The service provider may use the customer data of the subscribers referred to in subsection (1) sentence 2 for subscriber advisory purposes, for promoting his own offerings and for market research only to the extent required for such purposes and provided the subscriber has given his consent. A service provider who, under an existing customer relationship, has lawfully received notice of a subscriber's telephone number or postal address, including his electronic address, may use these for the transmission of text or picture messages to a telephone or postal address for the purposes referred to in sentence 1, unless the subscriber has objected to such use. Use of the telephone number or address according to sentence 2 shall be permitted only if the subscriber, when the telephone number or address is collected or first stored and on each occasion a message is sent to such telephone number or address for one of the purposes referred to in sentence 1, is given information in clearly visible and well readable form that he may object at any time, in writing or electronically, to the dispatch of further messages.

(3) When the contractual relationship ends, the customer data are to be erased by the service provider upon expiry of the calendar year following the year in which the contract terminated. Section 35(3) of the Federal Data Protection Act applies accordingly.

(4) In connection with the establishment of, or modification to, a contractual relationship or with the provision of telecommunications services, the service provider may require presentation of an official identity card where this is necessary to verify the subscriber's particulars. The service provider may make a copy of the identity card. The copy is to be destroyed by the service provider without undue delay once the particulars needed for the conclusion of the contract have been established. The service provider may not use data other than the data permitted under subsection (1).

(5) The provision of telecommunications services may not be made dependent upon the subscriber's consent to use of his data for other purposes where the subscriber is not able, or is not able in reasonable manner, to access such telecommunications services in another way.

Section 96

Traffic Data

(1) The service provider may collect and use the following traffic data to the extent required for the purposes set out in this Chapter–

1. the number or other identification of the lines in question or of the terminal, personal authorisation codes, additionally the card number when customer cards are used, additionally the location data when mobile handsets are used;

2. the beginning and end of the connection, indicated by date and time and, where relevant to the charges, the volume of data transmitted;

3. the telecommunications service used by the user;

4. the termination points of fixed connections, the beginning and end of their use, indicated by date and time and, where relevant to the charges, the volume of data transmitted;

5. any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes.

(2) Stored traffic data may be used after the termination of a connection only where required to set up a further connection or for the purposes referred to in sections 97, 99, 100 and 101. Otherwise, traffic data are to be erased by the service provider without undue delay following termination of the connection.

(3) The service provider may use subscriber-related traffic data used by the provider of a publicly available telecommunications service for the purpose of marketing telecommunications services, shaping telecommunications services to suit the needs of the market or for the provision of value added services for the duration necessary only where the data subject has given his consent to such use. The data of the called party are to be made anonymous without undue delay. Traffic data relating to the destination number may be used by the service provider for the purpose referred to in sentence 1 only with the consent of the called party. In such case, the called party data are to be made anonymous without undue delay.

(4) When obtaining consent, the service provider is to inform the subscriber of the data types which are to be processed for the purposes referred to in subsection (3) sentence 1 and of the storage duration. Additionally, the subscriber's attention is to be drawn to the possibility of withdrawing his consent at any time.

Section 97

Charging and Billing

(1) Service providers may use the traffic data set out in section 96(1) to the extent the data are required to charge and bill their subscribers. Where a service provider provides his services over the public telephone network of a third-party operator, such operator may transmit to the service provider the traffic data collected for the provision of his services. A service provider entering into a contract with a third party on the collection of charges may transmit to the third party the data referred to in subsection (2) to the extent required for collection of the charges and preparation of a detailed bill. The third party shall undertake contractually to maintain telecommunications privacy according to section 88 and data protection according to sections 93 and 95 to 97, 99 and 100. Section 11 of the Federal Data Protection Act remains unaffected.

(2) The service provider may, for proper telecommunications service charging and billing and verification of the accuracy of the same, collect and use the following personal data subject to the provisions of subsections (3) to (6)–

1. traffic data according to section 96(1);

2. the address of the subscriber or recipient of the bill, the type of line, the total number of units of use incurred during the accounting period for a regular bill, the volumes of data transmitted, the total amount payable;

3. other relevant billing information such as advance payments, payments with date of entry, payments in arrears, reminders, disconnections and restorations, complaints submitted and handled, extensions of time for payment applied for and granted, payment by instalment and provision of security.

(3) The service provider shall, after termination of the connection, establish from the traffic data according to section 96(1) paras 1 to 3 and 5 without undue delay the data required for charging. All data not required shall be erased without undue delay. Traffic data may – subject to subsection (4) sentence 1 para 2 – be stored for a period not exceeding six months after dispatch of the bill. Where, prior to expiry of the time limit referred to in sentence 3, the subscriber has raised objections to the amount billed, the traffic data may be stored until such time as the objections have been finally settled.

(4) Depending on how the subscriber chooses, the service provider issuing the bill shall, in respect of the destination number,

1. store it in full or with deletion of the last three digits; or

2. erase it completely upon dispatch of the bill to the subscriber.

The subscriber shall be informed of his right to choose; if he does not exercise this right, destination numbers shall be stored without deletion of the last three digits. Where a subscriber is liable to pay, in full or in part, the charges for incoming calls on his line, the numbers of the calling lines may be transmitted only with deletion of the last three digits. Sentences 1 and 2 do not apply to service providers offering their services solely to the members of closed user groups.

(5) The service provider may use traffic data to the extent required for his billing with other service providers or with their subscribers, and for other service providers' billing with their subscribers.

(6) Where the bill from the service provider includes payment for third-party services supplied in connection with the provision of telecommunications services, the service provider may transmit to the third party customer data and traffic data to the extent that these are required in a given instance to enforce third-party claims in relation to the subscriber.

Section 98

Location Data

(1) Location data relating to users of public telecommunications networks or publicly available telecommunications services may be processed only when they have been made anonymous or with the consent of the subscriber to the extent and for the duration necessary for the provision of value added services. The subscriber shall inform his co-users of all such consent given. Consent may be withdrawn at any time.

(2) Where the consent of the subscriber to the processing of location data has been obtained, the subscriber shall continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

(3) In respect of calls to the emergency call number "112", to telephone numbers determined in the ordinance as provided for under section 108(2) and to the telephone number "124124", the service provider shall ensure that the transmission of location data is not ruled out on a per-call or a per-line basis.

Section 99

Itemised Billing

(1) The subscriber shall be informed of data stored under section 97(3) sentences 3 and 4 and subsection (4) until dispatch of the bill and relating to calls for which he is liable to pay only if he has made a request, in text form, for an itemised bill prior to the relevant accounting period. In respect of residential lines, the disclosure of such information is permitted only if the subscriber has declared, in text form, that he has informed all co-users of the line, and will inform future co-users without undue delay, of the disclosure to him of the traffic data underpinning the bill. In respect of lines in businesses and public authorities, the disclosure of such information is permitted only if the subscriber has declared, in text form, that the employees have been informed, and new employees will be informed without undue delay, and that the works council or the staff representation has been involved in accordance with the statutory requirements, or that such involvement is not necessary. Where public-law religious societies have issued their own employee representation regulations for their domain, sentence 3 applies, it being understood that the respective employee representation acts in place of the works council or the staff representation. Furthermore, the subscriber may be informed of data stored under section 97(3) sentences 3 and 4 and subsection (4) after dispatch of the bill if he has raised objections to the amount billed. Where a subscriber is liable to pay, in full or in part, the charges for incoming calls on his line, the numbers of the calling lines may appear on the itemised bill issued to him only with deletion of the last three digits. Sentence 6 does not apply to service providers who, as providers for closed user groups, offer their services solely to the members of these.

(2) The itemised bill according to subsection (1) sentence 1 may not allow calls to persons, public authorities or organisations in the social or the church domain who or which offer anonymous counselling wholly or predominantly by telephone to callers in emotional or social distress and who or which themselves or whose employees therefore have a special duty not to disclose confidential information, to be identified. This applies only to the extent that the Regulatory Authority has entered such called lines on its register. Serving to provide counselling as defined in sentence 1, besides the groups referred to in section 203(1) paras 4 and 4a of the Penal Code, are, notably, telephone crisis counselling services and healthcare organisations. The Regulatory Authority enters the holders of these lines on its register, upon application, when they have evidenced their remit as set out in sentence 1 by certification from a public authority or corporation, a public-law agency or foundation. The register is kept available for retrieval in an automated procedure. The service provider shall access the register every quarter and incorporate in his billing procedures any changes without undue delay. Sentences 1 to 6 do not apply to service providers who, as providers for closed user groups, offer their services solely to the members of these.

(3) Customer cards, where used, shall carry clear indication of the possible disclosure of stored traffic data. Where such indication is not possible for technical reasons or could not reasonably be expected of the card issuer, the subscriber must have made a declaration according to subsection (1) sentence 2 or 3.

Section 100

Faults in Telecommunications Systems and Telecommunications Service Fraud

(1) Where required, the service provider may collect and use the customer data and traffic data of subscribers and users in order to detect, locate and eliminate faults and malfunctions in telecommunications systems.

(2) For purposes of changed implementations and the identification and location of faults in the network, the operator of the telecommunications system and his authorised representative shall be allowed to break in on existing connections, as far as this is operationally required. Break in shall be indicated by means of an acoustic signal and explicitly notified to the parties concerned.

(3) Where required, the service provider may collect and use the customer data and traffic data needed to detect and put a stop to the surreptitious use of services and other unlawful use of telecommunications networks and services when there are grounds, to be recorded in writing, to suppose such use. For the purpose referred to in sentence 1 the service provider may use collected traffic data in such a way as to identify, from the total traffic data not more than six months old, the data relating to those network connections in respect of which there are grounds to suppose that unlawful use of telecommunications networks and services has been made. In particular, the service provider may set up a pseudonymised data file from the customer data and the traffic data collected under sentence 1 which provides information on the revenues generated by the individual subscribers and which, suitable fraud criteria being applied, allows network connections in respect of which there are grounds to suppose that surreptitious use of services has been made, to be found. Data relating to all other communications are to be erased without undue delay. The Regulatory Authority and the Federal Data Protection Commissioner are to be notified without undue delay of the introduction of, and any modification to, the procedure according to sentence 1.

(4) Subject to the conditions referred to in subsection (3) sentence 1 the service provider may, in a given instance, collect and use control signals to the extent that this is indispensable to clarify and put a stop to the acts specified there. Collection and use of any other communications content is not permitted. The Regulatory Authority is to be notified of measures according to sentence 1 taken in a given instance. The parties concerned are to be advised as soon as it is possible to do so without the purpose of the measures being compromised.

Section 101

Information on Incoming Calls

(1) The service provider shall, upon written application, give any subscriber arguing conclusively in a procedure for documentation that he is the object of malicious or nuisance calls, information, for more than one network also, on the lines on which the calls originated. The information may relate solely to calls made after submission of the application. The service provider may collect, use and disclose to his subscriber data relating to the telephone numbers, names and addresses of the line holders and the date and time of the beginning of the calls and

call attempts. Sentences 1 and 2 do not apply to service providers offering their services solely to the members of closed user groups.

(2) Disclosure according to subsection (1) sentence 3 may be made only when the subscriber has narrowed down the calls beforehand in respect of date, time or any other suitable criteria if misuse of this procedure cannot be ruled out in any other way.

(3) In the case of information for more than one network, the other service providers contributing to the connection are obliged to give the service provider of the subscriber receiving malicious or nuisance calls the information required, provided they have such data.

(4) The holder of the line on which the identified calls originated is to be advised that information on these has been disclosed. An exception may be made if the applicant has argued conclusively in writing that any such disclosure could bring him significant disadvantages, and these disadvantages, when compared with the legitimate interests of the calling parties, appear considerably more serious. Subscribers on whose line the alleged malicious or nuisance calls originated receiving notice in another way of the disclosure of information are to be informed, upon request, of such disclosure.

(5) The Regulatory Authority and the Federal Data Protection Commissioner are to be notified without undue delay of the introduction of, and any modification to, the procedure to enforce subsections (1) to (4).

Section 102

Line Identification Presentation and Restriction

(1) Where the service provider offers calling line identification presentation, the calling and the called parties shall have the possibility, using a simple means and free of charge, of preventing presentation of the telephone number on a per-line or a per-call basis. Called parties shall have the possibility, using a simple means and free of charge, of rejecting incoming calls from a calling party that has prevented presentation of its telephone number. Sentences 1 and 2 do not apply to service providers offering their services solely to the members of closed user groups.

(2) Upon application by the subscriber, the service provider shall provide lines on which presentation on the connected line of the telephone number of the calling line is ruled out, free of charge. At the subscriber's request, these lines are to be indicated as such in the public directory of subscribers (section 104) issued by his provider. Where an indication according to sentence 2 has been made, presentation of the telephone number of the calling line on a line thus indicated shall be possible only when the indication has been taken out of the latest edition of the public directory.

(3) Where the subscriber has chosen not to apply for entry as provided for by section 104 in the directory of subscribers, presentation of the telephone number of his line shall not be made on the connected line unless the subscriber explicitly wishes such presentation.

(4) Where connected line identification presentation is offered, called parties shall have the possibility, using a simple means and free of charge, of preventing presentation of the connected line identification to the calling party. Subsection (1) sentence 3 applies accordingly.

(5) Subsections (1) and (4) also apply to calls to and from other countries, to the extent that they concern calling or called parties in the Federal Republic of Germany.

(6) In respect of calls to the emergency call number "112", to telephone numbers determined in the ordinance as provided for under section 108(2) and to the telephone number "124124", the service provider shall ensure that calling line identification presentation is not ruled out on a per-call or on a per-line basis.

Section 103

Automatic Call Forwarding

The service provider shall undertake to give his subscribers the possibility, using a simple means and free of charge, of stopping calls being automatically forwarded to their terminal as a result of action taken by a third party, to the extent that this is technically feasible. Sentence 1 does not apply to service providers who, as providers for closed user groups, offer their services solely to the members of these.

Section 104

Directories of Subscribers

Subscribers may have their name, address and additional information such as occupation, branch and type of line entered in public printed or electronic directories, where requested. Subscribers may specify what information is to be published in the directories. At the subscriber's request, co-users may be entered, provided they agree.

Section 105

Directory Information

(1) Information on telephone numbers included in directories may be provided subject to the restrictions set out in section 104 and in subsections (2) and (3).

(2) Information provided by means of a telephone system on the telephone numbers of subscribers may be given only if subscribers have been suitably informed that they may withhold consent to their telephone number being passed on and have not exercised their right to withhold consent. Information on data published under section 104 other than telephone numbers may be provided only if the subscriber has given his consent to such additional data being passed on.

(3) Providing information by means of a telephone system on the names or names and addresses of subscribers in relation to whom solely the telephone number is known is permitted if the subscriber whose data have been included in a directory of subscribers has not withheld consent after having been informed by his service provider of the possibility of doing so.

(4) All withholding of consent as provided for by subsection (2) sentence 1 and subsection (3) or giving of consent as provided for by subsection (2) sentence 2 shall be noted without undue delay in the customer files of the service provider or of the information provider according to subsection (1) on which the directories are based. Withholding or giving of consent shall also be heeded by the other service providers as soon as they could reasonably be

expected to know that the withholding or giving of consent has been noted in the directories of the service provider and of the information provider according to subsection (1).

Section 106

Telegram Service

(1) Data and documents relating to the operational handling and the delivery of telegrams may be stored to the extent necessary to demonstrate proper provision of the telegram service under the contract concluded with the subscriber. The data and documents shall be erased by the service provider after a period of six months at the latest.

(2) Data and documents relating to the content of telegrams may be stored beyond the date of delivery only if the service provider is answerable for transmission faults under the contract concluded with the subscriber. Data and documents relating to inland telegrams shall be erased by the service provider after a period of three months at the latest, and data and documents relating to international telegrams shall be erased by the service provider after a period of six months at the latest.

(3) The time limits for erasure shall begin running on the first day of the month following that in which the telegram was tendered. Erasure may be suspended where the prosecution of claims or international agreements necessitate a longer storage period.

Section 107

Store and Forward Systems

(1) In respect of services the carrying out of which requires intermediate storage, the service provider may process the content of communications, notably the voice, sound, text and graphics messages of subscribers, as part of a service offer based on these, subject to the following conditions–

1. processing takes place solely in telecommunications systems of the service provider carrying out intermediate storage, unless the content of the communication is re-routed to the telecommunications systems of other providers at the request of the subscriber or by subscriber input;

2. solely the subscriber determines, by his input, the content, scope and type of processing;

3. solely the subscriber determines who may input and access the content of communications (party having the right of access);

4. the service provider may inform the subscriber that the recipient has accessed the message;

5. the service provider may erase the content of communications only as provided for in the contract concluded with the subscriber.

(2) The service provider is to take the necessary technical and organisational measures to rule out transmission errors and the unauthorised disclosure, within his undertaking or to third parties, of the content of communications. Measures are required only if the time and effort expended is proportionate to the purpose of protection sought. Measures are to be adjusted to the state of the art if this is necessary to achieve the purpose of protection sought.

Chapter 3
Public Safety

Section 108
Emergency Calls

(1) Any person offering publicly available telephone services shall undertake to provide all users with access to emergency services by using, free of charge, the single European emergency call number "112" and the additional national emergency call numbers determined in the ordinance as provided for under subsection (2) sentence 1 para 1. Any person operating telecommunications networks used for publicly available telephone services shall be required to transmit to the local emergency service centre, without undue delay, emergency calls, including

1. the calling line identity or, where the calling line identity is not available, the data required to prosecute any misuse of emergency calls as provided for by the ordinance under subsection (2); and

2. the information required to identify the location from which the emergency call originated.

(2) The Federal Ministry of Economics and Labour shall be empowered to make arrangements by ordinance having the force of law and requiring the consent of the German Bundesrat, in agreement with the Federal Ministry of the Interior and the Federal Ministry of Health and Social Security, concerning

1. determination of the additional national emergency call numbers;

2. the setting up of emergency connections either as calls or telefaxes to the local emergency service centre;

3. the extent of the emergency call features to be provided by network operators for the single European emergency call number "112" and for the national emergency call numbers, including the provision and transmission of the information required to locate the emergency caller;

4. the provision and transmission of suitable data to enable emergency service centres to prosecute any misuse of emergency calls;

5. the setting up of emergency calls by means of automatic calling equipment; and

6. the responsibilities of the Regulatory Authority in the fields referred to in paras 2 to 5.

Federal state regulations on emergency service centres remain unaffected by the provisions of this subsection insofar as they do not relate to obligations for network operators within the meaning of subsection (1).

(3) The Regulatory Authority shall stipulate the technical details of the subject matter referred to in subsection (2) sentence 1 paras 2 to 5 in a technical directive to be drawn up with the participation of industry associations, the representatives of the emergency service centre operators nominated by the Federal Ministry of the Interior, and manufacturers. International

standards are to be taken into consideration; reasons for deviations from the standards are to be stated. The technical directive is to be published by the Regulatory Authority in its Official Gazette. All persons with obligations under subsection (1) sentence 2 are to meet the requirements of the technical directive not later than one year following its publication, unless a longer transitional period has been specified there for particular obligations. In the event of an amendment to the directive, defective-free technical facilities configured to the directive shall meet the modified requirements not later than three years following its taking effect.

Section 109

Technical Safeguards

(1) Every service provider shall make appropriate technical arrangements or take other measures in order to protect

1. the privacy of telecommunications and personal data; and

2. telecommunications and data processing systems against unauthorised access.

(2) Any person operating telecommunications systems serving to provide publicly available telecommunications services shall, additionally, make appropriate technical arrangements or take other measures in order to protect telecommunications and data processing systems operated for such purpose against any faults which would result in considerable harm to telecommunications networks, and against external attacks and the effects of natural disasters. In doing so, regard shall be had to the state of the art and to the physical location of own and shared network elements. Where a site or technical facilities are shared, each operator of the telecommunications system shall meet the obligations according to subsection (1) and sentence 1 unless particular obligations can be assigned to a particular operator. Technical arrangements and other safeguards are deemed reasonable if the technical and economic effort required is proportionate to the importance of the rights to be protected and to the importance of the facilities to be protected for the general public.

(3) Any person operating telecommunications systems serving to provide publicly available telecommunications services shall nominate a security commissioner and draw up a security concept setting out

1. which telecommunications systems are to be used and which publicly available telecommunications services provided;

2. any potential hazards, and

3. which technical arrangements or other safeguards have been made or put in place or are planned in order to meet the obligations according to subsections (1) and (2).

The security concept is to be submitted to the Regulatory Authority by the operator without undue delay after the beginning of provision of the telecommunications services, along with a declaration that the technical arrangements and other safeguards specified there have been, or will be, implemented without undue delay. Where the Regulatory Authority establishes shortcomings in the security concept itself or in the course of its implementation, it may require the operator to eliminate them without undue delay. If the configuration of the system on which the security concept is based changes, the operator shall adapt and resubmit his concept to the Regulatory Authority with reference to the changes made. Sentences 1 to 4 do not apply to

operators of telecommunications systems intended exclusively for the reception and distribution of broadcasting signals. The obligation according to sentence 2 is deemed met in respect of security concepts submitted to the Regulatory Authority under section 87 of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120).

Section 110

Technical Implementation of Intercepts

(1) Any person operating a telecommunications system by means of which publicly available telecommunications services are provided, shall,

1. from the time of beginning operation, at his own expense, provide technical facilities with which to implement telecommunications interception measures provided for by law and make organisational arrangements for the implementation, without undue delay, of such measures;

2. without undue delay after beginning operation, vis-à-vis the Regulatory Authority,

   a) declare that he has made the arrangements according to para 1; and

   b) nominate a body located in the Federal Republic of Germany to receive judicial orders destined for him, relating to telecommunications interception;

3. demonstrate to the Regulatory Authority, at no charge, that the technical facilities and organisational arrangements according to para 1 are compliant with the provisions of the ordinance according to subsection (2) and the technical directive according to subsection (3); to this end, he shall, without undue delay but not later than one month after beginning operation,

   a) send to the Regulatory Authority the documents needed to prepare the checks the Regulatory Authority carries out to verify compliance; and

   b) agree with the Regulatory Authority a date for demonstrating and verifying compliance;

   he shall assist the Regulatory Authority in the checks required for verifying compliance;

4. allow the Regulatory Authority, at its special request in a given, justified instance, to re-check, at no charge, his technical and organisational arrangements; and

5. tolerate the installation and operation on his premises of equipment for the implementation of measures under sections 5 and 8 of the Article 10 Act and grant staff of the office responsible for such measures and members and staff of the G10 Commission (section 1(2) of the Article 10 Act) access to such equipment for the discharge of their legal functions.

Any person offering publicly available telecommunications services without themselves operating a telecommunications system to do so shall, when choosing the operator of the telecommunications system to be used for doing so, make certain that the latter can carry out judicial orders relating to telecommunications interception without undue delay as provided for by the ordinance according to subsection (2) and by the technical directive according to subsection (3), and notify the Regulatory Authority without undue delay after beginning to provide service of which telecommunications services he is offering, by whom judicial intercept

orders concerning his subscribers are to be carried out and to which body located in the Federal Republic of Germany judicial orders relating to telecommunications interception are to be addressed. Any changes in the data on which the notifications according to sentence (1) para (2) b) and sentence 2 are based are to be notified to the Regulatory Authority without undue delay. In cases in which provisions according to subsection (3) are not yet available, the person with obligations shall configure the technical facilities according to sentence 1 para 1 in agreement with the Regulatory Authority. Sentences 1 to 4 do not apply where the ordinance according to subsection (2) provides for exemptions with regard to the telecommunications system. Section 100b(3) sentence 1 of the Code of Criminal Procedure, section 2(1) sentence 3 of the Article 10 Act and the relevant state regulations on preventive telecommunications interception by the police remain unaffected.

(2) The Federal Government shall be empowered

1. to make arrangements concerning

   a) the technical essential requirements and the organisational key elements for the implementation of intercepts, including the implementation of intercepts by a person acting on behalf of the person with obligations;

   b) the extent of the arrangements in the technical directive according to subsection (3);

   c) demonstration of compliance as provided for by subsection (1) sentence 1 paras 3 and 4; and

   d) details of the obligation of tolerance as required by subsection (1) sentence 1 para 5; and

2. to determine

   a) the cases in which and the conditions under which compliance with certain technical requirements can be dispensed with on a temporary basis;

   b) that the Regulatory Authority may, for technical reasons, allow exemptions in respect of meeting particular technical requirements; and

   c) in respect of which telecommunications systems and associated service offers technical facilities need not be offered or organisational measures need not be taken, in derogation of subsection (1) sentence 1 para 1, on account of basic technical considerations or for reasons of proportionality,

by ordinance having the force of law and requiring the consent of the German Bundesrat.

(3) The Regulatory Authority shall stipulate, in a technical directive to be drawn up in consultation with the authorised bodies and with the participation of industry associations and manufacturers, the technical details required to guarantee a full record of telecommunications intercepts and for configuration of the point of handover to the authorised bodies. International technical standards are to be taken into consideration; reasons for deviations from the standards are to be stated. The technical directive is to be published by the Regulatory Authority in its Official Gazette.

(4) Any person manufacturing or distributing technical facilities for the implementation of intercepts may require the Regulatory Authority to verify, by testing the interworking of a type

sample with particular telecommunications systems, whether or not the legal and technical provisions of the ordinance according to subsection (2) and of the technical directive according to subsection (3) have been met. The Regulatory Authority may, after due assessment of the circumstances, allow deviations from the technical requirements on a temporary basis, provided that implementation of the intercepts is secured in principle and only insignificant adjustments to the technical facilities of the authorised bodies are required. The Regulatory Authority is to notify the manufacturer or distributor in writing of the test results. The test results are noted by the Regulatory Authority in connection with the demonstration of compliance of the technical facilities with the applicable technical provisions which the person with obligations is required to provide under subsection (1) sentence 1 para 3 or 4. Consent to the framework concepts presented by manufacturers given by the Federal Ministry of Economics and Labour prior to the entry into force of this provision is deemed notification within the meaning of sentence 3.

(5) Any person obliged under subsection (1) in conjunction with the ordinance according to subsection (2) to make arrangements is to meet the requirements of the ordinance and the technical directive according to subsection (3) not later than one year following their publication, unless a longer period has been determined there for particular obligations. Defective-free technical facilities configured to this directive for telecommunications services already offered by the person with obligations shall, in the event of an amendment to the directive, meet the modified requirements not later than three years following its taking effect. Where shortcomings in the technical or organisational arrangements of the person with obligations are found in the process of compliance according to subsection (1) sentence 1 para 3 being demonstrated or a re-check according to subsection (1) sentence 1 para 4 being made, the person with obligations is to eliminate such shortcomings within a reasonable period of time as provided for by the Regulatory Authority; where shortcomings are found during operations, notably when intercepts are carried out, the person with obligations is to eliminate such shortcomings without undue delay. If type samples have been tested under subsection (4) for the technical facilities and deadlines set for the elimination of shortcomings, the Regulatory Authority shall take these deadlines into account in its specifications on the elimination of shortcomings according to sentence 3.

(6) Every operator of a telecommunications system renting to third parties network termination points in his telecommunications system under his publicly available service offer shall undertake to make available to the bodies authorised by law to carry out telecommunications intercepts, without undue delay and as a matter of priority, at their request, network termination points for transmission of the information obtained under an intercept. The technical configuration of such termination points may be laid down in the ordinance according to subsection (2). With the exception of special tariffs or surcharges for priority or early provision or fault repair, the tariffs payable by the general public apply in respect of such provision and use. Any special contractually agreed discounts remain unaffected by sentence 3.

(7) Telecommunications systems operated by legally authorised bodies and by means of which intervention in the privacy of telecommunications or in network operation is to be brought about, are to be technically configured in agreement with the Regulatory Authority. The Regulatory Authority is to comment on the technical configuration within a reasonable period of time.

(8) Operators of telecommunications systems with obligations under sections 100a and 100b of the Code of Criminal Procedure are to prepare, and make available to the Regulatory Authority at no charge, annual statistics of intercepts carried out under these provisions. The presentation of these statistics may be detailed in the ordinance according to subsection (2). Operators shall not disclose the statistics to third parties. The Regulatory Authority shall

aggregate the data provided by the undertakings and publish the result in its Official Gazette annually.

(9) The Federal Government shall be empowered to make arrangements, by ordinance having the force of law and requiring the consent of the German Bundestag and the German Bundesrat, with regard to appropriate compensation to be paid to service providers for services supplied by them in

1. enabling intercepts under sections 100a and 100b of the Code of Criminal Procedure, section 2(1), section 5 or section 8 of the Article 10 Act, section 39 of the Foreign Trade and Payments Act or the relevant state regulations, and

2. providing information in accordance with section 113.

The costs of providing technical facilities as required to provide the services according to sentence 1 are not the subject of such compensation arrangements.

Section 111

Data for Information Requests from Security Authorities

(1) Any person commercially providing or assisting in providing telecommunications services and in so doing allocating telephone numbers or providing telecommunications connections for telephone numbers allocated by other parties is, for the information procedures according to sections 112 and 113, to collect, prior to activation, and store without undue delay the telephone numbers, the name and address of the allocation holder, the effective date of the contract, the date of birth in the case of natural persons, and in the case of fixed lines, additionally the address for the line, even if such data are not required for operational purposes; where known, the date of termination of the contract is likewise to be stored. Sentence 1 also applies where the data are not included in directories of subscribers (section 104). A person with obligations according to sentence 1 receiving notice of any changes is to correct the data without undue delay; in this connection the person with obligations is subsequently to collect and store data according to sentence 1 not yet recorded if collecting the data is possible at no special effort. When the contractual relationship ends, the data are to be erased upon expiry of the calendar year following the year in which the contract terminated. Compensation for data collection and storage is not paid. The manner in which data for the information procedure according to section 113 are stored is optional.

(2) Where the service provider according to subsection (1) sentence 1 operates in conjunction with a sales partner, such partner shall collect data according to subsection (1) sentence 1 and transmit to the service provider, without undue delay, these and data collected under section 95; subsection (1) sentence 2 applies accordingly. Sentence 1 also applies to data relating to changes, inasmuch as the sales partner receives notice of them in the course of normal business transactions.

(3) Data within the meaning of subsection (1) sentence 1 need not be collected subsequently for contractual relationships existing on the date of entry into force of this provision, save in the cases referred to in subsection (1) sentence 3.

Section 112

Automated Information Procedure

(1) Any person providing publicly available telecommunications services shall store, without undue delay, data collected under section 111(1) sentences 1 and 3 and subsection (2) in customer data files in which the telephone numbers and quotas of telephone numbers allocated to other telecommunications service providers for further marketing or other use and, with regard to ported numbers, the current carrier portability codes, are also to be included. Section 111(1) sentences 3 and 4 apply accordingly with regard to the correction of customer data files. In the case of ported numbers the telephone number and associated carrier portability code are not to be erased before expiry of the year following the date on which the telephone number was returned to the network operator to whom it had originally been allocated. The person with obligations shall ensure that

1. the Regulatory Authority can, at all times, retrieve from customer data files data for information requests from the authorities referred to in subsection (2) by means of automated procedures in the Federal Republic of Germany;

2. data can be retrieved using incomplete search data or searches made by means of a similarity function.

The requesting office is to consider, without undue delay, the extent to which it needs the data provided and erase, without undue delay, any data not needed. The person with obligations is to ensure by technical and organisational measures that no retrievals can come to his notice.

(2) Information from the customer data files according to subsection (1) shall be provided to

1. the courts and criminal prosecution authorities;

2. federal and state police enforcement authorities for purposes of averting danger;

3. the Customs Criminological Office and customs investigation offices for criminal proceedings and the Customs Criminological Office for the preparation and execution of measures under section 39 of the Foreign Trade and Payments Act;

4. federal and state authorities for the protection of the Constitution, the Federal Armed Forces Counter-Intelligence Office and the Federal Intelligence Service;

5. the emergency service centres according to section 108 and the service centre for the maritime mobile emergency number "124124";

6. the Federal Financial Supervisory Authority; and

7. the authorities responsible under state legislation for the prosecution of administrative offences as provided for by section 4(3) of the Undeclared Work Act, via central inquiry offices,

as stipulated in subsection (4), at all times, as far as such information is needed to discharge their legal functions and the requests are submitted to the Regulatory Authority by means of automated procedures.

(3) The Federal Ministry of Economics and Labour shall be empowered to issue, in agreement with the Federal Chancellery, the Federal Ministry of the Interior, the Federal Ministry of Justice, the Federal Ministry of Finance and the Federal Ministry of Defence, an ordinance having the force of law and requiring the consent of the German Bundesrat, in which the following matters are regulated–

1. the essential requirements in respect of the technical procedures for

   a) the transmission of requests to the Regulatory Authority;

   b) the retrieval of data by the Regulatory Authority from persons with obligations, including the data types to be used for the queries; and

   c) transmission by the Regulatory Authority to the requesting authorities of the data retrieved;

2. the security requirements to be observed; and

3. in respect of retrievals using incomplete search data and searches made by means of similarity functions for which specifications on the character sequences to be included in the search are provided by the Ministries contributing to the ordinance,

   a) the minimum requirements in respect of the extent of the data to be entered in order to identify, as precisely as possible, the person to whom the search relates;

   b) the permitted number of hits to be transmitted to the requesting authority; and

   c) the requirements in respect of the erasure of data not needed.

In other respects, the ordinance may also restrict the query facility for the authorities referred to in subsection (2) paras 5 to 7 to the extent that is required for such authorities. The Regulatory Authority shall determine the technical details of the automated retrieval procedure in a technical directive to be drawn up with the participation of the associations concerned and the authorised bodies and to be brought into line with the state of the art, where required, and published by the Regulatory Authority in its Official Gazette. The person with obligations according to subsection (1) and the authorised bodies are to meet the requirements of the technical directive not later than one year following its publication. In the event of an amendment to the directive, defective-free technical facilities configured to the directive shall meet the modified requirements not later than three years following its taking effect.

(4) At the request of the authorities referred to in subsection (2), the Regulatory Authority is to retrieve and transmit to the requesting authority the relevant data sets from the customer data files according to subsection (1). It shall examine the admissibility of the transmission only where there is special reason to do so. Responsibility for such admissibility lies with the authorities referred to in subsection (2). For purposes of data protection control by the competent body, the Regulatory Authority shall record, for each retrieval, the time, the data used in the process of retrieval, the data retrieved, the person retrieving the data, the requesting authority and the reference number of the requesting authority. Use for any other purposes of data recorded is not permitted. Data recorded are to be erased after a period of one year.

(5) The person with obligations according to subsection (1) is to make all such technical arrangements in his area of responsibility as are required for the provision of information under

this provision, at his expense. This also includes procurement of the equipment required to secure confidentiality and protection against unauthorised access, installation of a suitable telecommunications connection, participation in the closed user system and the continued provision of all such arrangements as are required under the ordinance and the technical directive according to subsection (3). Compensation for information provided by means of automated procedures is not paid to persons with obligations.

Section 113

Manual Information Procedure

(1) Any person commercially providing or assisting in providing telecommunications services shall, in a given instance, provide the competent bodies, at their request, without undue delay, with information on data collected under sections 95 and 111 to the extent required for the prosecution of criminal or administrative offences, for averting danger to public safety or order and for the discharge of the legal functions of the federal and state authorities for the protection of the Constitution, the Federal Intelligence Service and the Federal Armed Forces Counter-Intelligence Office. The person with obligations according to sentence 1 shall provide information on data by means of which access to terminal equipment or to storage devices or units installed in such equipment or in the network is protected, notably personal identification numbers (PINs) or personal unlocking keys (PUKs), by virtue of an information request under section 161(1) sentence 1 or section 163(1) of the Code of Criminal Procedure, data collection provisions in federal or state police legislation for averting danger to public safety or order, section 8(1) of the Federal Constitution Protection Act, the corresponding provisions of the state constitution protection legislation, section 2(1) of the Federal Intelligence Service Act or section 4(1) of the Federal Armed Forces Counter-Intelligence Act; such data shall not be transmitted to any other public or private bodies. Access to data which are subject to telecommunications privacy shall be permitted only under the conditions of the relevant legislation. The person with obligations shall maintain silence vis-à-vis his customers and third parties about the provision of information.

(2) The person with obligations according to subsection (1) is to make such arrangements as are required in his area of responsibility for the provision of information, at his expense. In respect of information provided, the person with obligations is granted compensation by the requesting authority, the level of which, in derogation of section 17a(1) para 2 of the Reimbursement of Witnesses and Experts Act, is determined by the ordinance referred to in section 110(9). Sentence 2 also applies in those cases in which, under the manual information procedure, merely data are requested which the person with obligations also keeps available for retrieval under the automated information procedure according to section 112. Sentence 2 does not apply in those cases in which the information was not provided completely or was not provided correctly under the automated information procedure according to section 112.

Section 114

Information Requests from the Federal Intelligence Service

(1) Any person providing publicly available telecommunications services or operating transmission paths used for publicly available telecommunications services is to provide the Federal Ministry of Economics and Labour, upon request and at no charge, with information on the structures of telecommunications services and networks and on any forthcoming changes. Specific telecommunications activities and customer data of subscribers may not be the subject of any information under this provision.

(2) Requests for information according to subsection (1) are permissible only when a request for such information has been made by the Federal Intelligence Service and the information is required to discharge functions according to sections 5 and 8 of the Article 10 Act. Use of information obtained under this provision for any other purposes is ruled out.

Section 115

Monitoring and Enforcement of Obligations

(1) The Regulatory Authority may give orders and take other measures to secure compliance with the provisions of Part 7 and the ordinances having the force of law issued by virtue of this Part and with the applicable technical directives. The person with obligations shall provide the necessary information at the request of the Regulatory Authority. To verify compliance with obligations the Regulatory Authority is authorised to enter and inspect, during normal business or working hours, business premises and production sites.

(2) The Regulatory Authority may set the following financial penalties in accordance with the Administrative Enforcement Act–

1. a fine not exceeding 500,000 euros to enforce obligations according to section 108(1), section 110(1), (5) or (6), an ordinance according to section 108(2), an ordinance according to section 110(2), an ordinance according to section 112(3) sentence 1, the technical directive according to section 108(3), the technical directive according to section 110(3) and the technical directive according to section 112(3) sentence 3;

2. a fine not exceeding 100,000 euros to enforce obligations according to sections 109, 112(1) and (3) sentence 4, subsection (5) sentences 1 and 2 and section 114(1); and

3. a fine not exceeding 20,000 euros to enforce obligations according to section 111(1) sentences 1 to 4 and subsection (2) and section 113(1) and (2) sentence 1.

In the event of repeated violations of the provisions of section 111(1) sentences 1 to 4 and subsection (2), section 112(1) and (3) sentence 4, subsection (5) sentences 1 and 2 or section 113(1) and (2) sentence 1, the activities of the person with obligations may be restricted by order of the Regulatory Authority in such a way that his customer base may not be changed, except as a result of contract expiry or notice of termination, until such time as the obligations ensuing from these provisions have been fulfilled.

(3) In the event of the non-fulfilment of obligations set out in Part 7, the Regulatory Authority may, in addition, wholly or partially prohibit operation of the telecommunications system concerned or commercial provision of the telecommunications service concerned if less severe action to enforce proper conduct is insufficient.

(4) As far as the data of natural or legal persons are collected, processed or used for the commercial provision of telecommunications services, monitoring by the Federal Data Protection Commissioner as provided for by sections 21 and 24 to 26(1) to (4) of the Federal Data Protection Act shall apply in place of monitoring as provided for by section 38 of the Federal Data Protection Act in respect of undertakings. The Federal Data Protection Commissioner shall lodge his complaints with the Regulatory Authority and transmit to it any further results of monitoring after due assessment of the circumstances.

(5) The privacy of telecommunications as laid down in Article 10 of the Basic Law shall be restricted to the extent required for the monitoring specified in subsections (1) and (4).

PART 8

REGULATORY AUTHORITY

Chapter 1

Organisation

Section 116

Headquarters and Legal Status

(1) The Regulatory Authority for Telecommunications and Posts shall discharge the functions and exercise the powers assigned to it under this Act and other laws. The Regulatory Authority is a higher federal authority responsible to the Federal Ministry of Economics and Labour with its headquarters in Bonn.

(2) The Regulatory Authority shall be run by a President. The President shall represent the Regulatory Authority in and out of court and lay down the administration and order of business by rules of procedure; these shall require confirmation by the Federal Ministry of Economics and Labour. Section 132(1) remains unaffected.

(3) The President and the two Vice Presidents shall be nominated by the Federal Government upon the proposal of the Advisory Council. Where, in spite of a request from the Federal Government, the Advisory Council fails to make a proposal within a period of four weeks, the right of nomination shall end. In the event of a proposal from the Advisory Council failing to meet with the approval of the Federal Government, the Advisory Council may submit a further proposal within a period of four weeks. The right of the Federal Government to take the final decision remains unaffected by this procedure.

(4) The President and the two Vice Presidents shall be appointed by the President of the Federal Republic of Germany.

Section 117

Publication of Directives from the Federal Ministry of Economics and Labour

All directives issued by the Federal Ministry of Economics and Labour shall be published in the Federal Gazette. This does not apply to such functions as are to be discharged by the Federal Ministry of Economics and Labour under its own jurisdiction by virtue of this Act or other laws and the discharge of which it has transferred to the Regulatory Authority.

Section 118

Advisory Council

(1) There shall be constituted at the Regulatory Authority an Advisory Council. It shall consist of nine members of the German Bundestag and nine representatives of the German Bundesrat. The representatives of the German Bundesrat shall be members or political representatives of

the government of a federal state. The members and deputy members of the Advisory Council shall be appointed by the Federal Government upon the proposal of the German Bundestag and the German Bundesrat.

(2) Members proposed by the German Bundestag shall be appointed to the Advisory Council for the duration of the legislative period of the German Bundestag. They shall remain in office at the end of this legislative period until such time as the new members have been appointed. Reappointment is permitted. The representatives proposed by the German Bundesrat shall be appointed to the Advisory Council for a period of four years; reappointment is permitted. They shall be removed from office if the German Bundesrat proposes another person in their place.

(3) Members may ask the Federal Ministry of Economics and Labour to release them from service, and resign from office. The declaration of release requires written form. Members proposed by the German Bundestag shall lose their membership when the requirements for their appointment cease to apply.

(4) Should a member resign from office, a new member shall be appointed in his place without undue delay. Until such time as a new member has been appointed and in the event of a member being temporarily prevented from performing his duties, the appointed deputy shall discharge his functions. Subsections (1) to (4) apply to deputy members accordingly.

Section 119

Rules of Procedure, Chairmanship, Meetings of the Advisory Council

(1) The Advisory Council shall adopt its rules of procedure, which require the approval of the Federal Ministry of Economics and Labour.

(2) The Advisory Council shall elect a Chairman and a Deputy Chairman from its members in accordance with its rules of procedure. The candidate obtaining the majority of votes shall be elected. If the required majority is not achieved in the first ballot, the majority of votes cast shall decide in the second. In the event of a tie in the second ballot, the matter shall be resolved by drawing lots.

(3) The Advisory Council shall constitute a quorum whenever more than half of the members nominated by the German Bundesrat and by the German Bundestag respectively are present. Resolutions shall be adopted by simple majority. In the event of a tied vote, a motion shall be dismissed.

(4) Where the Chairman considers debate of a resolution in draft unnecessary, the approval or comments of the members can be obtained by means of a written enquiry. Subsection (3) applies accordingly with regard to resolutions being effected. The enquiry should be made sufficiently early so that, at the request of a member or of the Regulatory Authority, the matter can still be debated in timely manner at a meeting.

(5) The Advisory Council should meet at least once a quarter. Meetings are to be convened when the Regulatory Authority or at least three members make a written request for such convocation. The Chairman of the Advisory Council may convene a meeting at any time.

(6) Ordinary meetings are not open to the public.

(7) The President of the Regulatory Authority and persons authorised by him or her may attend the meetings. They shall be consulted at all times. The Advisory Council may require the presence of the President of the Regulatory Authority or, should the President be prevented from attending, that of a deputy.

(8) Members and persons representing them shall receive a refund of their travelling expenses and a commensurate attendance fee as determined by the Federal Minister of Economics and Labour.

Section 120

Functions of the Advisory Council

The Advisory Council shall have the following responsibilities–

1. making proposals to the Federal Government concerning the appointment of the President and Vice Presidents of the Regulatory Authority;

2. participating in Regulatory Authority decisions in the cases specified in section 61(4) paras 2 and 4 and section 81;

3. entitlement to request measures with which to implement the aims of regulation and to secure universal service. The Regulatory Authority shall undertake to decide on such requests within a period of six weeks;

4. entitlement in relation to the Regulatory Authority to obtain information and comments. The Regulatory Authority has the duty to provide information to the Advisory Council;

5. advising the Regulatory Authority in drawing up the Strategic Plan according to section 122(2) and, in particular, in making policy decisions of market relevance;

6. being consulted when the Frequency Usage Plan according to section 54 is drawn up.

Section 121

Activity Report

(1) The Regulatory Authority shall submit to the federal legislative bodies, along with the report according to subsection (2), a report on its activities and on the situation in and development of the telecommunications sector. This report shall also comment on the question of whether or not modification of the determination of which telecommunications services have been deemed universal services within the meaning of section 78 is recommended.

(2) The Monopolies Commission shall, every two years, prepare an official report assessing the level and foreseeable development of competition and the question of whether or not there are sustainable competitive telecommunications markets in the Federal Republic of Germany, evaluating the application of the provisions of this Act concerning regulation and fair trading and commenting on other current questions of competition policy, in particular, on the question of whether or not the ruling in section 21(2) para 3 needs to be adjusted in light of the development of competition. The report should be completed by 30 November of the year in which a main report according to section 44 of the Competition Act is not submitted.

(3) The Federal Government shall submit to the federal legislative bodies, within a reasonable period of time, its comments on the report.

Section 122

Annual Report

(1) Once a year, the Regulatory Authority shall publish a report on the development of the telecommunications market presenting the main market data and consumer protection issues.

(2) To be included in the Annual Report, after public consultation, is a Strategic Plan listing matters of legal and economic policy to be addressed by the Regulatory Authority in the current year. The findings are to be published in the Annual Report for the following year.

(3) The Regulatory Authority shall publish the principles of its administration on a regular basis.

Section 123

Cooperation with Other Authorities

(1) In the cases specified in sections 10, 11, 61(3) and section 62(2) para 3 the Regulatory Authority shall take decisions in agreement with the Federal Cartel Office. Where the Regulatory Authority takes decisions in accordance with Part 2, Chapters 2 to 5, it shall give the Federal Cartel Office the opportunity to state its views in good time before closure of the case. Where the Federal Cartel Office opens cases in the telecommunications sector under sections 19 and 20(1) and (2) of the Competition Act, Article 82 of the EC Treaty or section 40(2) of the Competition Act, it shall give the Regulatory Authority the opportunity to state its views in good time before closure of the case. Both authorities shall seek to achieve a uniform interpretation of this Act and one which is consistent with the Competition Act. They are to inform each other of all observations and findings which may be of significance to the discharge of their respective functions.

(2) The Regulatory Authority shall work together with the state media authorities. At their request, the Regulatory Authority shall inform these authorities of findings required for the discharge of their functions.

Section 124

Mediation

Where appropriate, the Regulatory Authority may, to resolve telecommunications disputes, propose that the parties affected seek to reach mutual agreement before a mediator (mediation process).

Section 125

Specialist Consulting

(1) The Regulatory Authority may set up special commissions to prepare its decisions or to deliver opinions on regulatory issues. The members of such commissions shall, in the field of

telecommunications or postal services, have particular experience of economic, business management, socio-political, technological and legal matters, and possess proven expertise.

(2) The Regulatory Authority shall be given, on a continuing basis, specialist support in performing its functions. This concerns, in particular,

1. the regular assessment of national and international economic, business management, regulatory and social trends in telecommunications and postal services; and

2. the preparation and further development of the scientific basis for shaping universal service, the regulation of providers with significant market power, the rules governing open network provision and interconnection as well as numbering and customer protection.

Chapter 2

Powers

Section 126

Prohibition

(1) Where the Regulatory Authority finds that an undertaking is failing to meet its obligations by or under this Act, it shall require the undertaking to state its views and to take remedial action. It shall set a time limit for the undertaking to take remedial action.

(2) Where the undertaking fails to meet its obligations within the time limit set, the Regulatory Authority may order such measures as are necessary to secure adherence to the obligations. A reasonable time limit is to be set to allow the undertaking to comply with the measures.

(3) In the case of serious or repeated breaches of obligations by the undertaking or failure to comply with measures for remedial action ordered by the Regulatory Authority under subsection (2), the Regulatory Authority may prohibit the undertaking acting in the capacity of telecommunications network operator or service provider.

4) Where such breach of obligations represents a direct and serious threat to public safety and order or such neglect of duty will create serious economic or operational problems for other providers or users of telecommunications networks or services, the Regulatory Authority may, in derogation of the procedures set out in subsections (1) to (3), take provisional measures. The Regulatory Authority shall decide, after it has given the undertaking concerned the opportunity to state its views within a reasonable period, whether the provisional measures will be confirmed, withdrawn or modified.

(5) To enforce orders according to subsection (2), a penalty not exceeding 500,000 euros may be set in accordance with the Administrative Enforcement Act.

Section 127

Information Requests

(1) Without prejudice to other national reporting or information requirements, public telecommunications network operators and providers of publicly available telecommunications services are obliged, under the rights and obligations ensuing from this Act, to provide the

Regulatory Authority, upon request, with information required for execution of this Act. The Regulatory Authority may, in particular, require information for

1. the systematic or case-by-case verification of compliance with obligations ensuing from or by virtue of this Act;

2. the case-by-case verification of compliance with obligations when the Regulatory Authority has received a complaint or has other reasons to assume non-compliance with obligations or when it has opened investigations on its own initiative;

3. the publication of comparative overviews of quality and price of service for the benefit of end-users;

4. clearly defined statistical purposes;

5. market definition or market analysis procedures according to sections 10 and 11;

6. procedures for the grant of rights of use and for the review of the relevant applications; and

7. the use of numbers.

Information as referred to in sentence 3, paras 1 to 5 may not be required prior to, or as a condition of, market access.

(2) As far as is necessary to discharge functions assigned to it under this Act, the Regulatory Authority may require telecommunications undertakings as referred to in subsection (1)

1. to provide information on their economic situation, in particular on their sales figures; and

2. to allow their business records to be inspected and audited within normal business or working hours.

(3) The Regulatory Authority shall request information as referred to in subsections (1) and (2) and arrange an audit as referred to in subsection (2) para 2 by written order. The legal basis, the subject matter and the purpose of the information request are to be stated in such order. In all information requests a reasonable time limit shall be determined for provision of the information.

(4) Owners of undertakings or persons representing them and, in the case of legal persons, corporations or associations without legal capacity, those persons appointed representatives by law or statutes, are obliged to provide information requested under subsections (1) and (2), to submit business records and to tolerate the auditing of their business records and access to business premises and property during normal business or working hours.

(5) Persons commissioned by the Regulatory Authority to conduct audits may have access to the offices and business premises of undertakings and associations of undertakings during normal business or working hours.

(6) Searches may be carried out solely by order of the local court in whose district the search is to take place. With regard to appeals against such orders, sections 306 to 310 and 311a of the Code of Criminal Procedure apply accordingly. In cases of imminent danger, the persons designated in subsection (5) may carry out, during business hours, the necessary searches

without a judicial order. On site, a record of the search and its main findings shall be drawn up, from which, where a judicial order was not obtained, the facts leading to the assumption of imminent danger are also apparent.

(7) Objects and business records may be taken into custody as required or, where they are not handed over voluntarily, seized. With regard to seizure, subsection (6) applies accordingly.

(8) Persons with obligations to provide information under subsection (4) may refuse to answer any questions which would render themselves or relatives as specified in section 383(1) paras 1 to 3 of the Code of Civil Procedure liable to prosecution or to proceedings under the Administrative Offences Act. Knowledge or records obtained as a result of information requests or measures according to subsections (1) and (2) may not be used for taxation assessment proceedings or administrative fines proceedings involving an offence against tax laws or currency violations or for proceedings involving a fiscal or currency offence; sections 93, 97, 105(1), section 111(5) in conjunction with section 105(1) and section 116(1) of the Fiscal Code do not apply in this regard. Sentence 1 does not apply in respect of proceedings involving a fiscal offence or any related taxation assessment proceedings when there is an overriding public interest in the institution of such proceedings, or in the event of the intentional provision of false information by persons with obligations or by persons acting on their behalf.

(9) As far as audits reveal a violation of any conditions, orders or directions of the Regulatory Authority, the undertaking is to reimburse the Regulatory Authority with the expenses, including any fees for experts, incurred by such audits.

(10) To enforce such orders, the Regulatory Authority may set a penalty not exceeding 500,000 euros in accordance with the Administrative Enforcement Act.

Section 128

Investigations

(1) The Regulatory Authority may conduct all investigations and take all evidence necessary.

(2) With regard to real evidence, testimonies and expert opinions, section 372(1), sections 376, 377, 380 to 387, 390, 395 to 397, 398(1) and sections 401, 402, 404, 406 to 409, 411 to 414 of the Code of Civil Procedure apply accordingly; detention may not be imposed. The higher regional court shall have jurisdiction to decide upon appeals.

(3) A record of the statements of the witnesses should be drawn up, to be signed by the investigating member of the Regulatory Authority and by a registrar also, if present. The record should include the place and date of the proceedings and the names of those assisting and of the parties concerned.

(4) The record is to be read to witnesses for their approval or presented for their own inspection. Approval given is to be noted and signed by the witnesses. In the event of the record not being signed, the reason is to be stated.

(5) With regard to the questioning of experts, subsections (3) and (4) apply accordingly.

(6) The Regulatory Authority may request the local court to administer an oath to witnesses if it deems an oath necessary to bring about true statements. The court shall decide upon such confirmation by oath.

Section 129

Seizure

(1) The Regulatory Authority may seize objects which may be important as evidence in its investigations. Any such seizure is to be notified to the parties concerned without undue delay.

(2) The Regulatory Authority is, within a period of three days, to seek judicial confirmation from the local court of the district in which seizure took place when neither the parties concerned nor adult relatives were present when seizure took place or when the parties concerned or, in their absence, adult relatives, expressly objected to such seizure.

(3) The parties concerned may at any time seek a judicial decision against seizure. They shall be instructed of this right. The court having jurisdiction according to subsection (2) shall decide on the motion.

(4) Appeals against judicial decisions are permissible. Sections 306 to 310 and 311a of the Code of Criminal Procedure apply accordingly.

Section 130

Provisional Orders

The Regulatory Authority may issue provisional orders pending a final decision.

Section 131

Conclusion of Proceedings

(1) Decisions of the Regulatory Authority are to be accompanied by a statement of reasons. They are to be served, along with the explanatory statement and information on permissible appeals, upon the parties concerned in accordance with the provisions of the Service in Administrative Procedure Act. Decisions issued in relation to an undertaking with its headquarters outside the area of application of this Act shall be served upon those designated by the undertaking and notified to the Regulatory Authority as persons authorised to accept service. Where the undertaking has not designated any such persons, the Regulatory Authority shall serve the decision by means of notice in the Federal Gazette.

(2) The closure of all proceedings not concluded by means of a decision served in accordance with subsection (1) sentences 2 to 4 upon the persons concerned is to be notified in writing to the persons concerned.

(3) The Regulatory Authority may charge the persons concerned with the cost of taking evidence as appears fair.

Chapter 3
Proceedings

Subchapter 1
Ruling Chambers

Section 132
Ruling Chamber Decisions

(1) The Regulatory Authority shall take decisions through its Ruling Chambers in the cases specified in Part 2, in section 55(9) and in sections 61, 62 and 81; subsection (3) sentence 1 remains unaffected. Decisions shall be taken by administrative act. Ruling Chambers shall, with the exception of the Chamber referred to in subsection (3), be constituted as provided for by the Federal Ministry of Economics and Labour.

(2) Chamber decisions shall be taken in the composition of Chairman and two Assessors. The Chairman and the Assessors shall be qualified to hold office in the senior administrative grade of the civil service. At least one member of the Ruling Chamber shall be qualified to exercise the functions of a judge.

(3) In the cases specified in section 55(9) and in sections 61, 62 and 81 the Ruling Chamber shall take decisions in the composition of the President as Chairman and the two Vice Presidents as Assessors; accordingly, subsection (2) sentences 2 and 3 do not apply as far as these cases are concerned. The authority to act as a deputy in cases of absence is regulated in the rules of procedure referred to in section 116(2). Decisions in the cases specified in section 61(4) paras 2 and 4 and in section 81 shall be taken in consultation with the Advisory Council.

(4) For the purposes of achieving a uniform ruling practice in comparable and related cases and of securing the consistency requirement according to section 27(2), procedures are to be stipulated in the Regulatory Authority's rules of procedure imposing extensive coordination and information obligations on the Ruling Chambers and the departments concerned prior to decisions being issued. Where Ruling Chamber decisions under sections 18, 19, 20, 21, 24, 30, 39, 40 and 41(1) are concerned, the rules of procedure shall ensure that determinations according to sections 10 and 11 are made by the President's Chamber.

Section 133
Other Disputes between Undertakings

(1) In the event of a dispute arising in connection with obligations ensuing from or by virtue of this Act between undertakings operating public telecommunications networks or offering publicly available telecommunications services, the Ruling Chamber shall, unless otherwise provided for by law, at the request of either party and after consultation with the parties concerned, issue a binding decision to resolve the dispute. The Ruling Chamber shall take its decision within a period not exceeding four months from the date of the request from one of the parties concerned to resolve the dispute.

(2) In the event of a dispute arising in a field covered by this Act between undertakings in different Member States where the dispute falls within the competence of the national regulatory authorities of at least two Member States, any of the parties may refer the dispute to the national

regulatory authority concerned. The Ruling Chamber is to take its decision in consultation with the national regulatory authority concerned within a period as referred to in subsection (1).

(3) Sections 126 to 132 and 134 to 137 apply accordingly.

Section 134

Institution of Proceedings, Parties Concerned

(1) Ruling Chambers shall institute proceedings on their own initiative or upon a motion.

(2) There shall take part in proceedings before the Chamber

1. the person presenting the motion;

2. the operators of public telecommunications networks and the providers of publicly available telecommunications services against whom the proceedings are directed; and

3. the persons and associations of persons whose interests are likely to be affected by the decision and to whom the Regulatory Authority has sent a summons to attend proceedings in response to their request.

Section 135

Hearings, Oral Proceedings

(1) The Chamber is to give parties concerned the opportunity to state their views.

(2) Where appropriate, the Chamber may give persons representing business circles affected by the proceedings the opportunity to state their views.

(3) The Chamber shall decide on the matter in question on the basis of public oral proceedings; subject to the agreement of the parties concerned, it can take its decision without oral proceedings. At the request of any of the parties concerned or on the Chamber's own initiative the public is to be excluded from part or all of the proceedings if it poses a threat to public order, specifically to national security, or to an important trade or operating secret.

Section 136

Trade and Operating Secrets

Without undue delay when documents are submitted for Ruling Chamber proceedings, all parties concerned are to mark those parts containing trade or operating secrets. In this case they shall submit an additional copy which, from their point of view, can be inspected without such secrets being disclosed. Where this does not happen, the Ruling Chamber may assume their agreement to inspection, unless it is aware of any special circumstances that do not justify such assumption. Where the Ruling Chamber considers marking the documents as confidential to be unjustified, it shall, prior to taking a decision on allowing inspection by third parties, consult with the submitting parties.

Subchapter 2

Legal Proceedings

Section 137

Appeals

(1) Protests and action against Regulatory Authority decisions shall not have suspensory effect.

(2) In the case of section 132, there shall be no preliminary proceedings.

(3) In the case of section 132, appeals (on issues of fact and law) against judgments and appeals (on procedural issues) against other decisions of the administrative court shall be ruled out. This does not apply with regard to appeals against decisions according to section 138(3), appeals against denial of leave to appeal on questions of law under section 135 in conjunction with section 133 of the Code of Administrative Court Procedure and appeals against decisions on jurisdiction under section 17a(2) and (3) of the Courts Constitution Act. Section 17a(4) sentences 4 to 6 of the Courts Constitution Act apply accordingly with regard to appeals against decisions on jurisdiction.

Section 138

Submission and Information Duties of the Regulatory Authority

(1) Section 99(1) of the Code of Administrative Court Procedure applies with regard to the submission of documents or files, the transmission of electronic documents and the provision of information (submission of documents) by the Regulatory Authority. The Regulatory Authority shall act in place of the supreme supervisory authority.

(2) Upon the motion of a party, the court dealing with the main issue shall decide by order whether the documents are to be submitted or whether they may not be submitted. Where trade or operating secrets will be affected as a result of the submission of documents according to subsection (1), the court shall require the authority to submit the documents insofar as this is of relevance to the decision, there are no other ways of clarifying the matter and, after due assessment of all the circumstances of the particular case, the interest in submission of the documents outweighs the interest in confidentiality of the person concerned.

(3) The motion is to be filed within a period of one month of the notification by the court to the parties concerned of the Regulatory Authority's decision on submission of the documents. The Regulatory Authority is to submit the documents at the court's request; section 100 of the Code of Administrative Court Procedure does not apply. The members of the court have a duty to observe secrecy; the reasons for the decision may not allow the nature or content of confidential documents to be ascertained. The court's decision on whether the documents are to be submitted or whether they may be submitted is appealable to the Federal Administrative Court. The appellate court division dealing with the main issue shall decide on the appeal. Sentences 2 and 3 apply accordingly with regard to the appeal proceedings.

(4) If, under the court's unappealable decision, the documents are not to be submitted or may not be submitted, the court or, in appeal proceedings, the court of appeal, shall return the documents submitted under subsection (3) sentence 2 to the Regulatory Authority immediately.

The court decision shall not be based on the content of any such documents unless all the parties concerned have given their consent.

Section 139

Participation of the Regulatory Authority in Civil Proceedings

Section 90(1) and (2) of the Competition Act apply accordingly with regard to civil proceedings ensuing from this Act. In all such cases the Regulatory Authority and its President shall act in place of the Federal Cartel Office and its President.

Subchapter 3

International Affairs

Section 140

International Affairs

The Regulatory Authority shall act on behalf of the Federal Ministry of Economics and Labour in the field of European and international telecommunications policy, in particular as regards participation in European and international institutions and organisations. This does not apply in respect of functions discharged by the Regulatory Authority under its own jurisdiction by virtue of this Act or other laws or by virtue of regulations of the European Communities.

Section 141

Recognised Accounting Authority in the Maritime Mobile Service

(1) The Federal Ministry of Economics and Labour shall be empowered to stipulate, by ordinance having the force of law but not requiring the consent of the German Bundesrat, the requirements and the procedure for recognition as a recognised accounting authority in the international maritime mobile service as provided for by the International Telecommunication Union. The procedure shall also specify the conditions for denial or revocation of such recognition.

(2) The authority responsible for the recognition of accounting authorities in the area of application of this Act shall be the Regulatory Authority.

PART 9

CHARGES

Section 142

Fees and Expenses

(1) The Regulatory Authority shall charge fees and expenses for the following official acts–

1. decisions on the grant of rights of use for frequencies according to section 55;

2. decisions on the grant of rights of use for telephone numbers by virtue of the ordinance according to section 66(4);

3. processing of applications for the registration of diallers using premium rate numbers;

4. case-by-case coordination, advance publication, assignment and notification of satellite systems according to section 56;

5. other official acts closely related to decisions taken under paras 1 to 4;

6. measures to counteract violations of this Act or of ordinances having the force of law issued by virtue of this Act;

7. decisions on the transfer of rights of way according to section 69; and

8. activities in connection with the procedure for recognition as a recognised accounting authority in the international maritime mobile service according to section 141.

Fees and expenses are also payable when an application for performance of an official act as specified in sentence 1

1. is rejected for reasons other than that of the authority not being responsible for the matter in question; or

2. is withdrawn after the beginning, but prior to completion, of processing.

(2) The Federal Ministry of Economics and Labour shall be empowered to stipulate in greater detail, in agreement with the Federal Ministry of Finance, by ordinance having the force of law but not requiring the consent of the German Bundesrat, chargeable acts and the level of the fees, including the mode of payment. The fee scales are to be calculated in such a way as to recover the costs incurred by the official acts. The provisions of the Administrative Expenses Act apply additionally. In derogation of sentence 2, the fees payable for decisions on the grant of rights of use according to subsection (1) paras 1 and 2 are to be determined in such a way that they serve, as a steering mechanism, to secure optimal and efficient use of these commodities in line with the aims of this Act. Sentences 2 to 4 do not apply when numbers or frequencies of exceptionally great economic value are allocated by means of competitive or comparative selection procedures. The Federal Ministry of Economics and Labour may transfer to the Regulatory Authority the power referred to in sentence 1 by ordinance having the force of law, securing the arrangement on agreement between the authorities concerned when it does so. An ordinance as referred to in sentence 6, including its repeal, requires the agreement of the Federal Ministry of Economics and Labour and the Federal Ministry of Finance.

(3) In derogation of the provisions of the Administrative Expenses Act, ordinances as referred to in subsection (2) sentence 1 may regulate the following matters–

1. the extent of the expenses to be refunded; and

2. the fees payable in respect of revocation or withdrawal of a grant of rights of use according to subsection (1) paras 1 or 2 or of a transfer of rights of way according to subsection (1) para 7 where this is attributable to the parties concerned.

(4) Fees and expenses may be assessed until the close of the fourth calendar year following creation of the debt (limitation of assessment period). Where an application for cancellation of or modification to the assessment is submitted prior to expiry of the time limit, the running of the assessment period is interrupted until such time as an unappealable decision on the application has been taken. The right to payment of fees and expenses shall lapse at the close of the fifth calendar year following assessment (lapse of right to enforce payment). In other respects, section 20 of the Administrative Expenses Act applies.

(5) In the case of auctions according to section 61(5) a fee for the grant of rights of use according to subsection (1) para 1 shall be payable only when it exceeds the proceeds from the auction.

(6) Authorities responsible for the construction and maintenance of public ways may, within their area of responsibility, adopt arrangements under which solely fees and expenses that cover the administrative costs of issuing notices of consent according to section 68(3) to the use of public ways may be charged. Flat-rate fees are permitted.

Section 143

Frequency Usage Contribution Charges

(1) The Regulatory Authority shall levy annual contribution charges to recover costs it incurs for the management, control and enforcement of general assignments and rights of use for spectrum and orbit usage under this Act and the ordinances issued by virtue of this Act. This includes, in particular, costs incurred by the Regulatory Authority for the following activities–

1. the planning and further development of frequency usages, including the necessary measurements, tests and compatibility studies to secure efficient and interference-free use of frequencies; and

2. international cooperation, harmonisation and standardisation.

(2) Liable to make contributions are all those who have been assigned frequencies. The share of the costs shall be allocated to the separate user groups produced by frequency allocation, as far as possible on an expenditure-related basis. Within these groups, the costs shall be split in accordance with the use of frequencies. Contributions are also payable when a frequency is used by virtue of another administrative act or on a lasting basis without an assignment. This applies, in particular, with regard to rights granted before 1 August 1996, insofar as they include determinations on frequency usage.

(3) Not to be included in the costs to be recovered under subsection (1) are costs for which fees according to section 142 or fees according to section 16 of the Radio Equipment and

Telecommunications Terminal Equipment Act of 31 January 2001 (Federal Law Gazette Part I page 170) or fees or contributions according to sections 10 or 11 of the Electromagnetic Compatibility Act of 18 September 1998 (Federal Law Gazette Part I page 2882) or the ordinances issued by virtue of these provisions have already been levied.

(4) The Federal Ministry of Economics and Labour shall be empowered to determine, in agreement with the Federal Ministry of Finance, by ordinance having the force of law but not requiring the consent of the German Bundesrat, and as provided for by the above subsections, details of the category of persons liable to pay contribution charges, the rates of contribution charge and the procedure for the collection of contribution charges, including the mode of payment. The share of the costs attributable to public interest is to be taken into account in the form of a reduction in the level of contribution. The Federal Ministry of Economics and Labour may transfer to the Regulatory Authority the power according to sentence 1 by ordinance having the force of law, securing the arrangement on agreement between the authorities concerned when it does so.

Section 144

Telecommunications Contribution Charges

(1) Persons with obligations under section 6(1) and section 4 of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120) shall pay a contribution charge to offset costs incurred by the Regulatory Authority for measures to secure fair competition and to promote public telecommunications markets with sustainable competition and for the management, control and enforcement of rights and obligations ensuing from this Act and from ordinances issued and rights of use granted under this Act, unless such costs are otherwise covered by fees or contribution charges levied under this Act. This also includes costs incurred by exercise of the functions referred to in sentence 1 in respect of international cooperation. The share of the costs attributable to public interest is to be taken into account in the form of a reduction in the level of contribution.

(2) The relevant costs according to subsection (1) shall be split proportionately among the separate undertakings in accordance with their revenues from activities according to section 6(1) and levied by the Regulatory Authority as an annual contribution charge.

(3) Fees paid under the Telecommunications Licence Fees Ordinance of 28 July 1997 (Federal Law Gazette Part I page 1936) and fees taken into account under section 16(2) of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120) shall, insofar as they exceed the fees payable under section 16(1) of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120) for the grant of a licence and the fees payable under the ordinance issued by virtue of that Act for the administrative cost of the grant of a licence, count towards the contribution charge. Section 143(3) applies accordingly.

(4) The Federal Ministry of Economics and Labour shall be empowered to regulate, by ordinance having the force of law but not requiring the consent of the German Bundesrat, in agreement with the Federal Ministry of Finance, details of the collection of contribution charges, notably the distribution key and reference date, the minimum assessment, the splitting mechanism, including a suitable estimation procedure and a classification scheme for determining the relevant costs according to subsection (2), the obligation to provide information on sales, including a suitable procedure allowing for flat-rate payment, as well as payment deadlines, mode of payment and the level of penalties for late payment. The ordinance may also set out arrangements for the provisional determination of contribution charges. The Federal

Ministry of Economics and Labour may transfer to the Regulatory Authority the power according to sentence 1 by ordinance having the force of law, securing the arrangement on agreement between the authorities concerned when it does so. An ordinance according to sentence 3, including its repeal, shall require the agreement of the Federal Ministry of Economics and Labour and the Federal Ministry of Finance.

Section 145

Cost of Out-of-Court Dispute Resolution Procedures

Fees and expenses are payable for out-of-court dispute resolution procedures according to section 45(3) para 6. The level of the fee payable for resolution is determined as provided for by section 11(2) sentences 2 and 3 of the Court Costs Act. Sections 3 to 9 of the Code of Civil Procedure apply accordingly with regard to determination of the amount in dispute. Where the dispute resolution office submits a proposal for resolution, it shall rule on the costs, having regard to the findings of fact and the matter in dispute, as appears fair. The cost ruling should be made along with the dispute resolution proposal. Each party shall bear the costs it has incurred for participation in the procedure itself. In other respects, sections 8 to 21 of the Administrative Expenses Act apply accordingly.

Section 146

Cost of Preliminary Proceedings

Fees and expenses are payable for preliminary proceedings. A fee not exceeding the fee fixed for the contested official act is payable for the complete or partial rejection of a protest. Where a fee is not payable for the contested official act of the Regulatory Authority, the fee is determined as provided for by section 11(2) sentences 2 and 3 of the Court Costs Act; section 145 sentence 3 applies accordingly. Where a protest is withdrawn after processing has begun but prior to its completion, the fee shall not exceed 75 percent of the protest fee. The protests office shall decide the costs according to sentences 2 and 4 as appears fair.

Section 147

Information from the Regulatory Authority

The Regulatory Authority shall publish a yearly overview of its administrative costs and the total sum of charges collected. Where required, the fees and rates of contribution charges shall be adjusted for the future in the ordinances concerned.

PART 10
PENAL AND ADMINISTRATIVE FINES PROVISIONS

Section 148

Penal Provisions

(1) Any person who,

1. in contravention of section 89 sentence 1 or 2, intercepts a communication or imparts to others the content of a communication or the fact of its reception; or

2. in contravention of section 90(1) sentence 1,

   a) owns, or

   b) manufactures, markets, imports or otherwise introduces in the area of application of this Act

   transmitting equipment as referred to there,

is liable to a term of imprisonment not exceeding two years, or to a financial penalty.

(2) Where action in the cases of subsection (1) para 2 b) arises through negligence, the offender is liable to a term of imprisonment not exceeding one year, or to a financial penalty.

Section 149

Administrative Fines Provisions

(1) An administrative offence is deemed to have been committed by any person who, intentionally or negligently,

1. in contravention of section 4, fails to provide information, to provide it correctly, to provide it completely or to provide it in timely manner;

2. in contravention of section 6(1), fails to notify the Regulatory Authority, to notify it correctly, to notify it completely, to notify it as prescribed or to notify it in timely manner;

3. in contravention of section 17 sentence 2, passes on information;

4. contravenes an enforceable order according to

   a) section 20, section 23(3) sentence 2, section 29(1) sentence 1 para 1 or subsection (2) sentence 1 or 2, section 37(3) sentence 2, also in conjunction with section 38(4) sentence 4, section 38(4) sentence 2, also in conjunction with section 39(3) sentence 1 or section 42(4) sentence 1, also in conjunction with section 18(2) sentence 2;

   b) section 67(1) sentence 4 or section 109(3) sentence 3;

c) section 29(1) sentence 2, section 39(3) sentence 2, section 65 or section 127(2) para 1;

5. in contravention of section 22(3) sentence 1, fails to submit an agreement or to submit it in timely manner;

6. charges rates without approval as required under section 30(1) or section 39(1) sentence 1;

7. in contravention of section 38(1) sentence 1 or 3 or section 39(3) sentence 4, fails to inform the Regulatory Authority of rates or rate measures, to inform it correctly, to inform it completely or to inform it in timely manner;

8. in contravention of section 47(1), fails to provide subscriber data, to provide them correctly, to provide them completely or to provide them in timely manner;

9. in contravention of section 50(3) para 4, fails to notify the Regulatory Authority, to notify it correctly, to notify it completely or to notify it in timely manner;

10. uses a frequency without frequency assignment as required under section 55(1) sentence 1;

11. exercises German rights to orbit or frequency usage without assignment of such rights as required under section 56(1) sentence 1;

12. contravenes an enforceable condition according to section 60(2) sentence 1;

13. contravenes an ordinance according to section 66(4) sentence 1 or an enforceable order issued by virtue of such ordinance, insofar as the ordinance refers to this administrative fines provision in respect of a particular offence;

14. in contravention of section 87(1) sentence 1 or section 110(1) sentence 2 or 3, fails to inform or notify the Regulatory Authority, to inform or notify it correctly, to inform or notify it completely or to inform or notify it in timely manner;

15. in contravention of section 90(3), advertises transmitting equipment;

16. in contravention of section 95(2) or section 96(2) sentence 1 or subsection (3) sentence 1, uses data;

17. in contravention of section 96(2) sentence 2 or section 97(3) sentence 2, fails to erase data or to erase them in timely manner;

18. in contravention of section 106(2) sentence 2, fails to erase data and documents or to erase them in timely manner;

19. in contravention of section 108(1) sentence 1, also in conjunction with an ordinance according to section 108(2) sentence 1 para 1, fails to provide access to emergency services or to provide it as prescribed;

20. in contravention of section 108(1) sentence 2 in conjunction with an ordinance according to section 108(2) sentence 1 para 4, fails to transmit the data or information as referred to there or to transmit them in timely manner;

21. in contravention of section 109(3) sentence 2 or 4, fails to submit or to resubmit a security concept or to submit or to resubmit it in timely manner;

22. in contravention of section 110(1) sentence 1 para 1 in conjunction with an ordinance according to section 110(2) para 1 a), fails to provide a technical facility or to make organisational arrangements;

23. in contravention of section 110(1) sentence 1 para 2 b), fails to nominate a body as named there or to nominate it in timely manner;

24. in contravention of section 110(1) sentence 1 para 3, fails to demonstrate compliance or to demonstrate it in timely manner;

25. in contravention of section 110(1) sentence 1 para 4, fails to allow a re-check;

26. in contravention of section 110(1) sentence 1 para 5, fails to tolerate the installation or operation of equipment referred to there or to grant access to such equipment;

27. in contravention of section 110(5) sentence 3, fails to eliminate shortcomings or to eliminate them in timely manner;

28. in contravention of section 110(6) sentence 1, fails to make available a network termination point, to make it available as prescribed or to make it available in timely manner;

29. in contravention of section 111(1) sentence 1, also in conjunction with sentence 2, or in contravention of section 111(1) sentence 3 or 4, fails to collect data or to collect them in timely manner, fails to store data or to store them in timely manner, fails to correct data or to correct them in timely manner or fails to erase data or to erase them in timely manner;

30. in contravention of section 111(2) sentence 1, also in conjunction with sentence 2, fails to collect data or to collect them in timely manner or fails to transmit data or to transmit them in timely manner;

31. in contravention of section 112(1) sentence 4, fails to ensure that the Regulatory Authority can retrieve data from customer data files;

32. in contravention of section 112(1) sentence 6, fails to ensure that no retrievals can come to his notice;

33. in contravention of section 113(1) sentence 1 or 2, section 114(1) sentence 1 or section 127(1) sentence 1, fails to provide information, to provide it correctly, to provide it completely or to provide it in timely manner;

34. in contravention of section 113(1) sentence 2 second half-sentence, transmits data; or

35. in contravention of section 113(1) sentence 4, fails to maintain silence.

(2) Such offences may be punishable by a fine not exceeding five hundred thousand euros in the cases of an offence according to subsection (1) para 4 a), paras 6, 10, 22, 27 and 31, by a fine not exceeding three hundred thousand euros in the cases of an offence according to subsection (1) paras 16 to 18, 26, 29 and 34, by a fine not exceeding one hundred thousand euros in the cases of an offence according to subsection (1) para 4 b), paras 12, 13, 15, 19, 21

and 30, by a fine not exceeding fifty thousand euros in the cases of an offence according to subsection (1) paras 5, 7, 8, 9, 11, 20, 23 and 24, and by a fine not exceeding ten thousand euros in the other cases of offences according to subsection (1). The fine should exceed the economic benefit the offender has derived from the offence. Amounts as referred to in sentence 1 which are not sufficient for this may be exceeded.

(3) Administrative authority within the meaning of section 36(1) para 1 of the Administrative Offences Act shall be the Regulatory Authority.

PART 11

TRANSITIONAL AND FINAL PROVISIONS

Section 150

Transitional Provisions

(1) Determinations of market dominance made by the Regulatory Authority prior to the entry into force of this Act and the resulting obligations shall remain in effect until such time as they are replaced by new decisions taken in accordance with Part 2. This also applies when the determinations of market dominance merely constitute part of the statement of reasons for an administrative act. Sentence 1 applies accordingly with regard to obligations set out in sections 36, 37 and 39 second alternative of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120).

(2) Undertakings which have given notification under the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120) that they provide telecommunications services or are licensees shall, without prejudice to the obligation set out in section 144(1) sentence 1, not be subject to the notification requirement according to section 6.

(3) Existing frequency assignments, number allocations and rights of way granted under section 8 of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120) shall remain in effect. The same applies to rights acquired beforehand entitling the holder to use frequencies.

(4) Where frequency usage and licence rights have been granted in markets in which competitive or comparative selection procedures have been carried out, rights thus granted and obligations thus entered into shall continue. This applies, in particular, in respect of the obligation to admit service providers, applicable at the time the mobile licences were granted.

(5) Section 21(2) para 3 applies until 30 June 2008 subject to the proviso that wholesale line rental has to be made available only in conjunction with calls.

(6) Section 48(2) para 2 applies with regard to equipment placed on the market as from 1 January 2005.

(7) Until such time as a Frequency Usage Plan according to section 54 is issued, frequencies shall be assigned in accordance with the provisions of the applicable National Table of Frequency Allocations.

(8) Section 62(1) to (3) do not apply to rights granted under section 2(1) of the Telecommunication Installations Act as published on 3 July 1989 (Federal Law Gazette Part I

page 1455) or to licences granted or frequencies assigned under sections 10, 11 and 47(5) of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120) for the period of validity specified for such licences and frequencies.

(9) Where Deutsche Telekom AG intends not to offer universal services as specified in section 78(2) to the full extent or to offer them under less favourable conditions than those specified in this Act, it shall notify the Regulatory Authority of such intentions one year prior to their taking effect.

(10) The Telecommunications Interception Ordinance of 22 January 2002 (Federal Law Gazette Part I page 458), last amended by Article 328 of the Ordinance of 25 November 2003 (Federal Law Gazette Part I page 2304) applies in place of the ordinance according to section 110(2) until such time as this ordinance has entered into force.

(11) The technical directive issued under section 11 of the Telecommunications Interception Ordinance as amended at the time of entry into force of section 110 applies in place of the technical directive according to section 110(3) until such time as this directive has been issued.

(12) In respect of contractual relationships existing on the date of entry into force of this provision, persons with obligations under section 112(1) shall enter data they have to hand as a result of earlier data surveys without undue delay in customer data files according to section 112(1). In respect of contracts concluded after the entry into force of section 112, data which providers have not yet been able to include in a customer data file on account of the file structure used hitherto shall be included without undue delay following adaptation of the file. The interface specification published by the Regulatory Authority under section 90(2) and (6) of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120) as amended at the time of the entry into force of section 112 applies in place of the technical directive according to section 112(3) sentence 3 until such time as this directive has been issued.

(13) The admissibility of appeals against court decisions shall be decided in accordance with the provisions applicable to date if the court decision is pronounced prior to the entry into force of this Act or served ex officio instead of pronouncement.

(14) The provisions to date are applicable to motions submitted under section 99(2) of the Code of Administrative Court Procedure prior to the entry into force of this Act.

Section 151

Amendment of Other Legal Provisions

(1) The Code of Criminal Procedure as published on 7 April 1987 (Federal Law Gazette Part I pages 1047, 1319), last amended by Article 4(22) of the Act of 5 May 2004 (Federal Law Gazette Part I page 718) shall be amended as follows–

in section 100b(3) sentence 2 for the words "section 88 of the Telecommunications Act" there shall be substituted the words "section 110 of the Telecommunications Act".

(2) The Article 10 Act of 26 June 2001 (Federal Law Gazette Part I pages 1254, 2298), last amended by Article 4(6) of the Act of 5 May 2004 (Federal Law Gazette Part I page 718) shall be amended as follows–

1. in section 2(1) sentence 4 for the words "section 88 of the Telecommunications Act" there shall be substituted the words "section 110 of the Telecommunications Act";

2. section 20 shall read as follows–

"Section 20

Compensation

Bodies authorised under section 1(1) shall pay compensation for services according to section 2(1), the level of which shall be determined, in respect of measures for

a) postal intercepts, in accordance with section 17a of the Reimbursement of Witnesses and Experts Act; and

b) telecommunications intercepts, in accordance with the ordinance referred to in section 110(9)."

(3) Section 17a(1) para 3 subpara (1) second and third half-sentences and subsection (6) of the Reimbursement of Witnesses and Experts Act as published on 1 October 1969 (Federal Law Gazette Part I page 1756), last amended by Article 1(5) of the Act of 22 February 2002 (Federal Law Gazette Part I page 981) shall expire on the date of the entry into force of the ordinance according to section 110(9).

Section 152

Entry into Force, Expiry

(1) Subject to sentence 2, this Act shall enter into force on the day following its promulgation. Section 43(a) and (b), section 96(1) para 9 a) to 9 f) in conjunction with subsection (2) sentence 1 and section 97(6) and (7) of the Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120), last amended by Article 4(73) of the Act of 5 May 2004 (Federal Law Gazette Part I page 718) remain applicable in the version valid until the entry into force of this Act until such time as the ordinance according to section 66(4) of this Act has been issued. In respect of section 43b(2) this applies subject to the proviso that the pricing information requirement is no longer restricted to calls from the fixed network as from 1 August 2004.

(2) The Telecommunications Act of 25 July 1996 (Federal Law Gazette Part I page 1120), last amended by Article 4(73) of the Act of 5 May 2004 (Federal Law Gazette Part I page 718), the Television Signals Transmission Act of 14 November 1997 (Federal Law Gazette Part I page 2710), last amended by Article 222 of the Ordinance of 25 November 2003 (Federal Law Gazette Part I page 2304), the Telecommunications Rates Regulation Ordinance of 1 October 1996 (Federal Law Gazette Part I page 1492), the Network Access Ordinance of 23 October 1996 (Federal Law Gazette Part I page 1568), the Telecommunications Universal Service Ordinance of 30 January 1997 (Federal Law Gazette Part I page 141), section 4 of the Telecommunications Customer Protection Ordinance of 11 December 1997 (Federal Law Gazette Part I page 2910), last amended by the Ordinance of 20 August 2002 (Federal Law Gazette Part I page 3365), the Telecommunications Data Protection Ordinance of 18 December 2000 (Federal Law Gazette Part I page 1740), amended by Article 2 of the Act of 9 August 2003 (Federal Law Gazette Part I page 1590), the Frequency Assignment Ordinance of 26 April 2001 (Federal Law Gazette Part I page 829) and the Telecommunications Licence Fees Ordinance of 9 September 2002 (Federal Law Gazette Part I page 3542) shall expire on the day following the promulgation of this Act.

Hawrylak, Maciek

From: Durand, Mathieu
Sent: October-05-12 8:57 AM
To: Hawrylak, Maciek; Scott, Marcie; Maillé, Marie Anick; Chayer, Marie-Helene
Subject: Annual Report 2011-2012 on the Privacy Act & Lawful Access

Hello all,

FYI, the annual report of the Privacy commissioner for 2011-2012 is out. Here is a copy/paste of the section on lawful access:

Lawful Access

The interplay between privacy and security is a fundamental question to any open, democratic society. Our Office understands the need and the importance of integrating privacy protections into public safety measures.

The Investigating and Preventing Criminal Electronic Communications Act (Bill C-30), introduced in February 2012, is but the latest incarnation of a longstanding project by authorities to recast Canada's legal framework regulating use of electronic surveillance.

Our Office has had a lengthy history with this effort and our exchanges with government on it extend back as far as the mid-1990s.

Our Office understands the challenges faced by law enforcement and national security authorities in fighting online crime - especially in an era of evolving communications technologies.

However, legislation that seeks to recalibrate police powers online must demonstrably help protect the public, respect fundamental privacy principles established in Canadian law and be subject to proper oversight. It is a standard of Canada's approach to surveillance that the invasiveness of a new police power or investigative method must be offset by similar levels of legal review, accountability and oversight.

Canadians care passionately about their right to privacy. Citizens from all walks of life, from every part of the country, irrespective of age and upbringing connect instinctively with this issue.

And so, when the government is proposing new methods of electronic surveillance - and contemplating the ideal balance between effective security and meaningful privacy - the views of citizens must be taken into account.

Since 2005, we have made our concerns public in parliamentary submissions and statements, responses to government consultations, communiqués issued with our provincial and territorial privacy counterparts, as well as in letters to responsible Ministers and lead departments. We have articulated these same concerns in speeches before professional associations, conference presentations, discussion papers and even classroom lectures.

In October 2011, we sent an open letter to the Minister of Public Safety to once again articulate our deep concerns prior to the reintroduction of legislation.

The proper treatment of personal information and the safeguarding of citizen's rights and freedoms in the context of national security are among the government's most pressing duties. Privacy protection is not an ancillary issue in this domain, but at the heart of the social freedoms that governments are bound to safeguard.

To date, Canadians have not been given sufficient justification for the proposed new powers when other, less intrusive alternatives could be explored. A focused, tailored approach is vital.

In February 2012, the federal government introduced the latest version of lawful access legislation, which proposes to expand the legal tools of the state to conduct surveillance and access private information.

For many years, our Office has been urging a cautious approach to creating an expanded surveillance regime that would have serious repercussions for privacy rights. We are not convinced that the latest bill takes the focused, tailored approach necessary to avoid the erosion of our free, open society.

We do recognize that the government, in that bill, reduced the number of data elements which could be accessed by authorities without a warrant or prior judicial authorization. There were also certain oversight provisions included in the latest version of the bill.

On balance, however, the legislation contains serious privacy concerns, similar to past versions.

In particular, we are concerned about access, without a warrant, to subscriber information behind an **IP** address. Since this broad power is not limited to reasonable grounds to suspect criminal activity or to a criminal investigation, it could affect any law-abiding citizen.

The ongoing privacy issues that remain outstanding include:
- The scope of the new powers, which can be accessed by a wide range of provincial and federal authorities;
- Access to personal information without judicial authorization, including instances unrelated to crime or security issues;
- The lack of public reporting, which lessens accountability and complicates Parliamentary review; and
- The absence of dedicated review, to properly control and check on the use of new investigative tools.

We look forward to sharing our detailed views on this bill with Parliament when Bill C-30 is studied in Committee.

Hawrylak, Maciek

From: Durand, Mathieu
Sent: September-28-12 4:26 PM
To: Hawrylak, Maciek
Subject: Lawful Access in the US, France and the UK

Maciek,

Here is the link to the document. Do not hesitate to write on it (you have full ~~access~~ Power). As discussed, I suggest that you start reading at page 12.

Thank you again (et bon weekend)

Mathieu

Hawrylak, Maciek

From: Kwavnick, Andrea
Sent: September-28-12 9:15 AM
To: Hawrylak, Maciek
Subject: Lawful Access - PMR

s.16(2)
s.19(1)

Hi Maciek,

Once TBS informs you that the report has been approved, please send an email to the contacts in the email below simply stating that the LA PMR has been approved by TBS and that TBS will send out a formal letter to the agencies/depts. shortly.

Some of the addresses did not show up in the email below:

Francine Chartrand - Francine.Chartrand@ppsc-sppc.gc.ca
Tina Hattem - Tina.Hattem@ppsc-sppc.gc.ca

Please include Lisa Foley on the email as well. I had included Bruce on the Aug 20th email as [redacted]

Thanks
Andrea

From: Kwavnick, Andrea [mailto:Andrea.Kwavnick@ps-sp.gc.ca]
Sent: August 20, 2012 10:08 AM
To: [redacted] Nguyen, Trang Dai; Audcent, Karen; Shogilev, Matthew; [redacted] Chartrand, Francine; Hattem, Tina; Bruce.Wallace@ic.gc.ca; 'Andre.Leduc@ic.gc.ca' (Andre.Leduc@ic.gc.ca); Pierre Piché (pierre.piche@rcmp-grc.gc.ca); Sgt. Mark Flynn (mark.flynn@rcmp-grc.gc.ca); Kousha, Hasti; Cameron, Frank
Cc: Haeck, Kimberly
Subject: Lawful Access - Performance Measurement Report

Good Morning,

The PMR has been approved at the PS DG level (Director General of the National Security Operations Directorate) and is ready to be approved by your respective ADMs.

As indicated in the critical path that was sent out at the beginning of this process, please send me an email indicating ADM-level approval by Tuesday, August 28th.

It is necessary that approval be granted by August 28th in order to have sufficient time for the report to be approved by TBS before the September 15th deadline.

Please note that two small changes were made in the Introduction:

1 – pg. 8 - under Legislation/Policy Documents; second last line used to read "a significant portion of the policy work..." this was changed to "a significant portion of the regulatory work..."

2 – pg. 8 – under Consultation/Outreach; the following sentence was added: "Many partners also took part in discussions with representatives of the telecommunications industry through a Government Industry Collaborative Forum that was created in 2012."

Below are the ADM-level officials who signed off on the report last year. Please let me know if there have been any changes:

Antoine Babinsky - Royal Canadian Mounted Police
[redacted] Canadian Security Intelligence Service
- Communications Security Establishment Canada
Donald Piragoff - Department of Justice
George Dolhai - Public Prosecution Service Canada
Susan Bincoletto - Industry Canada

s.16(2)

RCMP/CSIS/CSEC – the report will be sent over secure email.
IC/PPSC/DoJ – please contact Kim Haeck to pick up a disk.

Thank you very much for your help putting this year's report together. Please give me a call if you have any questions.

Andrea

Andrea Kwavnick
Senior Policy Analyst, Investigative Technologies and Telecommunications Policy |
Conseillère principale en politiques, Technologies d'enquêtes et politiques des télécommunications
National Security Operations | Opérations de la sécurité nationale
Public Safety Canada | Sécurité publique Canada
613.949.6169 / Andrea.Kwavnick@ps.gc.ca

Department of Justice Canada | Ministère de la Justice Canada

MEMORANDUM / NOTE DE SERVICE

Security classification – Cote de sécurité
Protected B / Solicitor- Client Privilege
File Number – Numéro de dossier
61100-5-5
Date (Y-A / M / D-J)
2012-08-24
Telephone / Fax – Téléphone / Télécopieur
613-948-7418

TO / DEST. : Hasti Kousha, Counsel, Public Safety Canada Legal Services and Michèle Kingsley, Director, National Security Technologies, Public Safety Canada

FROM / ORIG. : Matthew Shogilev, Counsel, Criminal Law Policy Section (CLPS), Justice Canada (with input from Karen Audcent, Senior Counsel, CLPS and Joanne Klineberg, Senior Counsel, CLPS)

s.23

[redacted]

JUS 107 (2009/10)

Pages 485 to / à 487

are withheld pursuant to section

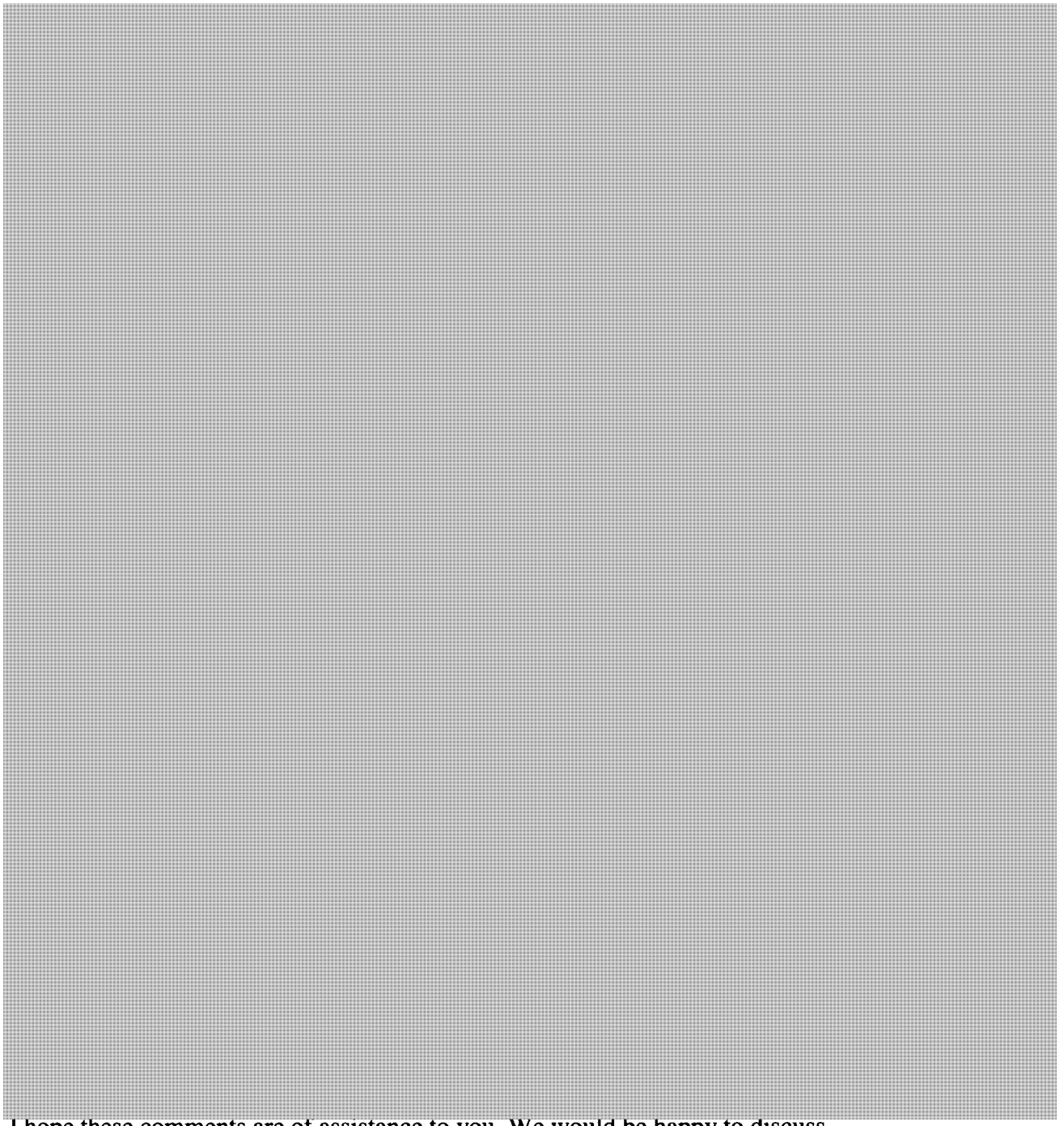
sont retenues en vertu de l'article

23

of the Access to Information

de la Loi sur l'accès à l'information

s.23



I hope these comments are of assistance to you. We would be happy to discuss.

Emmett, Jamie

From: Soper, Lesley <Lesley.Soper@pco-bcp.gc.ca>
Sent: August-09-12 4:35 PM
To: Kwavnick, Andrea
Cc: Maillé, Marie Anick; Kagedan, Allan
Subject: RE: Lawful Access

Thanks – much appreciated

Lesley Soper
Senior Analyst | Analyste principale
Security and Intelligence Secretariat |Secrétariat de la sécurité et du renseignment
Privy Council Office | Bureau du Conseil privé
59 rue Sparks Street
Ottawa K1A 0A3
613-957-5359
613-957-5277 (fax/télécopieur)

From: Kwavnick, Andrea [mailto:Andrea.Kwavnick@ps-sp.gc.ca]
Sent: August 9, 2012 4:26 PM
To: Soper, Lesley
Cc: Maillé, Marie Anick; Kagedan, Allan
Subject: Lawful Access

Lesley,

As requested, we are sending a list of groups who have publicly come out in support of Bill C-30. We are also including groups who have expressed support for Lawful Access legislation prior to the introduction of the Bill in 2012.

Please let us know if you require more information.

Thanks
Andrea

The following groups have publicly expressed support for Bill C-30:

Canadian Association of Chiefs of Police - www.cacp.ca/media/news/download/1246/Final_CACP_Press_Release_-_Lawful_Access_%28Final_English%29.pdf

Canadian Police Association - www.cpa-acp.ca/home/index_e.asp

CSIS - www.thestar.com/news/canada/politics/article/1225998--csis-chief-supports-online-surveillance-bill-offers-to-help-tweak-legislation

Vancouver Police Department - http://mediareleases.vpd.ca/2012/02/20/vpd-speaks-on-lawful-access-bill-c-30/

Calgary Police Service - http://www.calgarysun.com/2012/02/15/cops-defend-web-bill

Winnipeg Police Service - http://winnipeg.ca/police/press/2012/02feb/2012_02_17.stm

Ottawa Police Service - http://www.cfra.com/?nid=84492&cat=1

Halifax Regional Police - http://www.bedfordbeacon.com/hrp-supports-cacps-position-on-lawful-access

The following groups have publicly expressed support for Lawful Access legislation prior to the introduction of Bill C-30:

Federal/Provincial/Territorial Ministers of Justice and Public Safety (2012) – http://www.scics.gc.ca/english/conferences.asp?a=viewdocument&id=1701

Canadian Association of Chiefs of Police (2011) - http://www.cacp.ca/media/resolutions/efiles/38/Final_English_Resolutions_Adopted_2011.pdf (pg. 3-6)

Federal Ombudsman for Victims of Crime (2009) - http://www.victimsfirst.gc.ca/media/news-nouv/nr-cp/2009/20090618.html

Security Intelligence Review Committee (2009) - http://www.sirc-csars.gc.ca/pdfs/ar_2008-2009-eng.pdf (pg. 18-19)

Federal Ombudsman for Victims of Crime (2007) - - http://www.victimsfirst.gc.ca/pdf/childp-pjuvenile.pdf (pg. 15-23)

Canadian Resource Centre for Victims of Crime (2007) - http://crcvc.ca/docs/CONSULTATIONS_lawful%20access_Oct07.pdf

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
February 21, 2012

CACP Appeals to Canadians – The Lens of Law Enforcement

``Why we are asking for Lawful Access"

OTTAWA, ON – The Canadian Association of Chiefs of Police (CACP) is asking Canadians to consider the views of law enforcement as they debate what we refer to as ' lawful access', or Bill C-30 – *"An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts."*

President of the CACP, Chief Dale McFee: "The CACP has endorsed lawful access legislation since it was first introduced by government in 2002. Canadians more than understand the exponential growth in technology which has occurred over the last few decades. Yet, law enforcement is being asked to protect the communities we serve based on legislation introduced in 1975 - the days of the rotary phone."

The Global Internet, cellular phones and social media have been widely adopted and enjoyed by Canadians, young and old. Many of us have been affected by computer viruses, spam and increasingly, bank or credit card fraud. These new medias are also being used as a safe haven for serious criminal activity – identity theft, child and sexual exploitation, gangs, organized crime and national security threats.

"This is a huge challenge facing law enforcement agencies. We collectively need every reasonable tool to prevent such activity from happening in the first place or to investigate and lay charges when it does. We also need the privacy safeguards to ensure we're accountable in the use of these tools and Bill C-30 provides just that" states OPP Commissioner Chris Lewis."

"The debate – balancing community safety and privacy rights – is a debate which must occur and we are very mindful and respectful of the views of all Canadians. The CACP, however, is disappointed in the amount of misinformation and rhetoric that is clouding an important discussion on this issue. It stems from appealing to the greatest fears of Canadians and suggesting that law enforcement may misuse

such legislation. It has been propagated that law enforcement could freely monitor the 'surfing habits of Canadians' and do so without a warrant. "Nothing could be farther from the truth" states Vancouver D/Chief Warren Lemcke, who is also Chair of the CACP Law Amendments Committee.

Obtaining content or monitoring (tracking) communication requires a warrant and this condition remains with C-30. Basic subscriber information (BSI) is an on-going challenge for law enforcement to obtain. In some cases ISP's provide the information, others will not, or often there are lengthy delays. The RCMP's National Child Exploitation Centre states that "in 2010, the average response time for these requests was 12 days." During this time, victims continue to be victimized.

In its report *Every Image, Every Child – Internet-Facilitated Child Sexual Abuse in Canada* the Office of the Federal Ombudsman for Victims of Crime outlines the very serious issues faced by law enforcement. Canada's Federal Ombudsman for Victims of Crime, Sue O'Sullivan, further underlined the importance of the need for lawful access to Parliament 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*):

> *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.*

One example that demonstrates the need for this type of information (further examples are provided in the attached correspondence):

> 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.

The CACP believes that Bill C-30 provides greater oversight to obtain BSI than within the current environment. Today, obtaining basic subscriber information is completely ad hoc and uncontrolled. There is no certainty that basic information can be provided in a timely and consistent manner to law enforcement for investigative purposes.

"Under this new lawful access legislation, strict procedures for recording, reporting and auditing of all requests to obtain BSI are put in place. This information is documented and provided to senior Public Safety officials throughout Canada, including Privacy Commissioners. Those within law enforcement who can obtain BSI information is strictly limited. There is actually significantly more oversight with this legislation than what exists today" Chief McFee reaffirms.

To promote balanced discussion on this issue, the Canadian Association of Chiefs of Police have prepared a document entitled "Simplifying Lawful Access – Bill C-30." It is available on the CACP website (www.cacp.ca) or directly at (Link). The document compares today's environment versus that proposed under the new legislation, provides answers to 'frequently asked questions' and a series of Case Studies describing the utility of BSI to law enforcement (when it works and when it does not).

Our hope is that Members of Parliament, the media and Canadians as a whole will take the time to view the importance of this legislation through the lens of law enforcement.

The Canadian Association of Chiefs of Police (CACP) 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

Canadian Police Association

The national voice for Canadian police personnel

A Canadian Police Association Program "Leading Edge in Policing" Initiative A Closer Look at the Economics of Policing October 29-30, 2013

RATIONALE

There is a need for a forum at which leading edge research and police practice can be featured and discussed. This assumes even greater importance given the current discussions of the economics of

Read More...

PLEASE BE PATIENT, WE ARE CURRENTLY UPDATING OUR WEB SITE

QUOTABLES:

Harper government introduces Protecting Children from Internet Predators Act

"Without this legislation, we're asking our police to use pagers and typewriters to keep up with criminals using smart phones and tablets. We look forward to an engaged and responsible debate on this legislation, but we do hope that we can see this Bill passed as quickly as possible."

- Tom Stamatakis

Cops for Kids Safety

By raising awareness on law enforcement and justice issues, the CPA promotes community safety. Th...

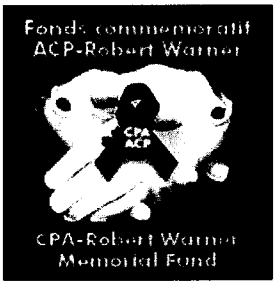
[Read More]

CPA-Robert Warner Memorial Fund

URGENT APPEAL

Help us help the families of police officers killed in the line of...

[Read More]



What's New

- CPA Attends Economics of Policing Summit... - (Posted 2/3/2013)
- Season's Greetings!... - (Posted 12/20/2012)
- CPA President Tom Stamatakis addresses the media's... - (Posted 8/22/2012)
- Second degree murder charge could have chilling ef... - (Posted 3/2/2012)
- Happy New Year!... - (Posted 1/1/2012)

[More News]

ECCO PARTNERS WITH THE CPA!

[redacted] The CPA is proud to announce a new partnership with ECCO Canada that will greatly benefit its members! ECCO is a worldwide known shoemaker founded in Denmark in 1963. Over the years they developed a technology, craftsmanship and insights that make shoes comfortable and stylish whether it is for work, golf or leisure time.

For more information click here!

The CPA Calendar of events/training is now online!

Click here to view the activities.

News / Canada

CSIS chief supports online surveillance bill, offers to help tweak legislation

Canada's spy chief backs the Conservative government's troubled bid to bolster Internet surveillance powers, and has offered to help tweak the legislation to make it more palatable to a wary public.

ADRIAN WYLD / THE CANADIAN PRESS

CSIS head Richard Fadden waits to testify at the Commons public safety committee on Parliament Hill in Ottawa, July 5, 2010. Fadden says the spy agency was "extremely pleased" to see the bill come before Parliament, considering it "vital" to protecting national security.

By:Jim Bronskill The Canadian Press, Published on Fri Jul 13 2012

OTTAWA—Canada's spy chief backs the Conservative government's troubled bid to bolster Internet surveillance powers, and has offered to help tweak the legislation to make it more palatable to a wary public.

In a letter to Public Safety Minister Vic Toews, Canadian Security Intelligence Service director Dick Fadden says the spy agency was "extremely pleased" to see the bill come before Parliament, considering it "vital" to protecting national security.

CSIS was drafting "potential options" to strengthen accountability measures in the bill, says the late February letter, sent to the embattled minister following a wave of opposition to the legislation from civil libertarians and Internet privacy advocates.

The Canadian Press obtained a declassified version of the top secret letter this week under the Access to Information Act.

The federal legislation would allow police, intelligence and competition bureau officers access to Internet subscriber information — including name, address, telephone number, email address and

Internet Protocol address — without a warrant. An IP address is the numeric label assigned to a computer on the Internet.

It would also require telecommunication service providers to have the technical capability to enable police and spies to intercept messages and conversations.

"Of the various provisions contained in the bill, the intercept capability requirements are of primary importance to the Service and critical to national security," Fadden says in the letter.

There have been cases in which such technical barriers prevented CSIS prevented from carrying out surveillance authorized by Federal Court warrant, he says. Operations are also jeopardized when communication networks "go dark" — including one unexpected outage that lasted over a week, Fadden adds.

The RCMP has said that police must often engineer interception solutions before they are able to execute a court order, meaning sometimes they are unable to tap into communications.

Fadden acknowledges the cost for companies to set up and maintain intercept-capable networks could be significant. But he argues the legislation provides "generous lead times and grandfathering provisions" that will help industry.

Opponents of the bill say allowing authorities access to Internet subscriber information without a court-approved warrant would be a dangerous infringement of privacy because even that limited data can be revealing.

"This is all stuff that can together give a pretty solid road map of what you are doing online and who you are talking to," said Lindsey Pinto, spokeswoman for OpenMedia.ca, which promotes an open, affordable Internet and has vociferously lobbied against the bill.

"Based on that kind of information, it is fairly easy to see what kind of website somebody is visiting, who they're in touch with, what their social media profiles are."

Fadden urged the government to address the issue.

"Concerning basic subscriber information (BSI), the Service would welcome any efforts to clarify that the content of users' communications, including web browsing, may still only be obtained with a warrant."

Still, Fadden says CSIS would lend a hand by drafting "potential options to strengthen the accountability regime on the BSI provisions of the bill."

Ultimately these provisions "would bring legislative clarity, predictability and accountability to an important investigative practice," Fadden adds.

CSIS spokeswoman Tahera Mufti said the spy service did provide advice to the minister but she declined to say more.

"I will not comment on the details of this exchange or further elaborate on our position with respect to this legislation."

When concerns about the bill arose in the Commons shortly before its introduction, Toews told a Liberal MP he could either stand with the government or "with the child pornographers" prowling online.

His comment drew widespread denunciation.

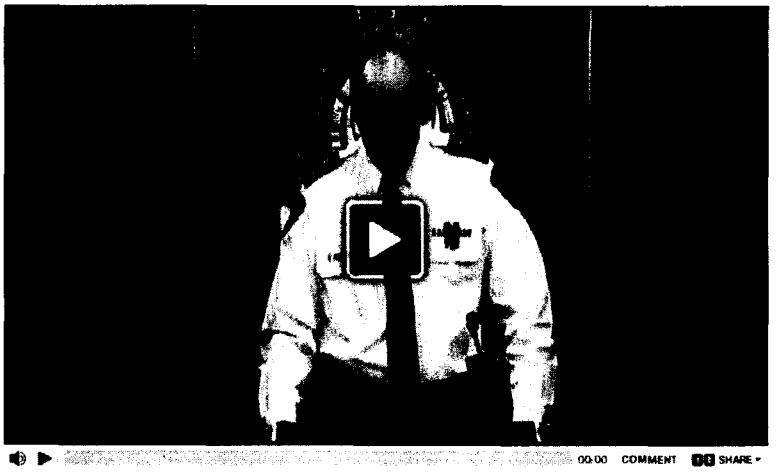
Amid the furor, the government indicated a willingness to amend the legislation by sending it straight to committee for study instead of the usual second reading in the House of Commons. However, the bill did not resurface before the Commons rose for the summer.

Fadden's letter makes it clear he is eager to see the legislation re-emerge.

"The Service remains available to support this process through all legislative stages and we view this legislation as vital in our ability to protect Canada's national security in a world of rapidly evolving technology."

VPD Speaks on Lawful Access – Bill C-30

February 20, 2012



Watch live streaming video from vancouverpolice at livestream.com

DEPUTY CHIEF WARREN LEMCKE
INVESTIGATION DIVISION
REMARKS

Today I speak to you as the Deputy Chief of the VPD's Investigation Division, but also as a member of the Canadian Association of Chiefs of Police, and I'm pleased to be joined by Tom Stamatakis, President of both the Vancouver Police Union and Canadian Police Association.

The Canadian Association of Chiefs of Police (CACP) is asking Canadians to consider the views of law enforcement as they debate what we refer to as "lawful access," or Bill C-30 – "An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts."

This Bill was introduced by government last week and it has generated much controversy. There is no doubt that the Bill is complex and the technology it refers to can be complex as well.

I would, however, like to try to provide some understanding of the Bill from a police perspective. 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 (i.e. suicide prevention, notifying next of kin, etc.)

The global internet, cellular phones and social media have all been widely adopted and enjoyed by Canadians, young and old. Many of us have been affected by computer viruses, spam and increasingly, bank or credit card fraud.

These new technologies are also being used as a safe haven for serious criminal activity – identity theft, child and sexual exploitation, gangs, organized crime and national security threats. This is a huge challenge facing law enforcement agencies.
We collectively need every reasonable tool to prevent such activity from happening in the first place or to investigate and lay charges when it does.

We also need the privacy safeguards to ensure we're accountable in the use of these tools and we believe Bill C-30 provides just that.

Current legislation regarding lawful access was drafted in 1975, in the days of the rotary phone. The proposed legislation will help the police deal with today's technological challenges that face law enforcement and, in some cases, hamper our ability to protect the public.

The legislation can be broken down into three main areas:

1. First there are the sections around intercept capability.

What this deals with is the fact that there are some telecommunication service providers (TSPs) who are in business in Canada who do not have the technological ability to provide information to police upon lawful request or with warrant.
What that means is that police could go to one of these providers with a warrant to intercept calls in a kidnapping investigation and they do not have the capability to allow us to do that.

This bill will require all TSPs to have the necessary infrastructure to allow police to get the data or intercepts they need when they are lawfully allowed to do so.
Lives could depend on this.

2. Secondly, the matter of basic subscriber information is particularly sensitive.

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 to police who are in the lawful execution of their duties.

While this information is important to police in all types of investigations, it can be 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 was in trouble or being victimized.

An example would be a message over the internet indicating someone was contemplating suicide where all we had was an email address.

Currently, there is no audited process for law enforcement to gain access to basic subscriber information. In some cases, internet service providers (ISPs) provide the information to police voluntarily — others will not, or often there are lengthy delays. The problem is that there is no consistency in providing this information to police nationally.

The RCMP's National Child Exploitation Centre states that, "In 2010, the average response time for these requests was 13 days." During this time, victims continue to be victimized.

Currently, law enforcement agencies are not directly accountable for these requests and for the information that they obtain. 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 ministers, privacy commissioners, federal and provincial authorities, etc.

3. Lastly, and one of the most important things to remember, this bill does NOT allow the police to monitor emails, phone calls or internet surfing at will without a warrant, as has been implied or explicitly stated.

There is no doubt that those who are against the legislation want you to believe that it does. I have read the Bill and I cannot find that anywhere in it. There are no changes in this area from the current legislation.

The new Bill does require that upon the request of a police office, a TSP must freeze data for 21 days while police get a warrant to examine that data. This is tremendously important as it does take time to get a warrant, and the preservation of data, preventing it from being erased, can be critical to catching a criminal.

There is nothing in the bill that authorizes the police to ask 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"). While it provides authority for police to obtain basic subscriber information in the course of their duties, access to email and internet activity is only available with a warrant, as is the case now.

This legislation is important to enhance the ability for police in Canada to investigate crime and prevent victimization. Our hope is that Members of Parliament, the media and Canadians as a whole will take the time to view this legislation through the lens of law enforcement.

The debate – balancing community safety and privacy rights – is a debate which must occur and we are very mindful and respectful of the views of all Canadians. The CACP, however, is disappointed in the amount of misinformation and rhetoric that is clouding an important discussion on this issue.

Other police officials across the country will be providing comment in the coming days as well.

Tweet 0

« Public Notification: Suspicious Vehicle
Suspicious Death »

Cops defend web bill

Police say laws need to catch up with the times

BY NADIA MOHARIB,CALGARY SUN

FIRST POSTED: WEDNESDAY, FEBRUARY 15, 2012 07:08 PM MST | UPDATED: WEDNESDAY, FEBRUARY 15, 2012 11:55 PM MST

FILE PHOTO

The federal bill aimed at increasing police access to online data, often key to police investigations, won't trample on privacy rights say supporters.

Wednesday, a day after the feds tabled the Internet Lawful Access Bill, Public Safety Minister Vic Toews said his government would "entertain amendments" to the bill.

The Conservative government went into full retreat after the bill created a public uproar over concerns it would infringe on privacy rights, but Calgary cops say the legislation has been misinterpreted.

Deputy Chief Murray Stooke said laws governing new technology, like the Internet, were created when there were still rotary phones, cablegrams and telegrams — long before the web, cell phones and GPS existed.

"We really need to modernize this area of the law," he said.

"We can't create safe havens where criminals can ply their trade."

Bill-30 would allow authorities without a warrant to force Internet service providers to reveal clients' names, addresses, phone numbers, email addresses, IP addresses as well as the name of any service provider.

Those changes, Stooke said, would see police more quickly able to clear a common hurdle at the onset of an investigation.

Getting basic information — from cell phone numbers, IP addresses and email address as the bill proposes — offers a starting point.

assaults and murders and wouldn't allow authorities to monitor an individual's Internet surfing habits or get into emails.

Cpl. Kimberley Krasman, with the Integrated Child Exploitation unit, said the changes are key to getting timely leads on investigations, especially ones where predators need to be stopped.

""It's not as nefarious as anybody makes it out to be," she said.

— With files by QMI Agency

nadia.moharib@sunmedia.ca

On Twitter @sunnadiamoharib

February 17, 2012

Winnipeg Police Service Media Release
For Immediate Release

Intelligence Directed Crime Prevention Strategy - Division 11

Due to the combined efforts of General Patrol members, the Community Support Unit, Foot Patrol Unit, Detectives, with the assistance of the Street Crimes Unit and the Tactical Support Unit, numerous individuals have been arrested in connection with a number of robberies and other serious incidents in the downtown area.

This has been a result of an INTELLIGENCE DIRECTED CRIME PREVENTION STRATEGY and is part of the continued commitment to the Downtown Safety initiative.

This working group looked at a number of factors and determined hotspot (s) within the division, resulting in a coordinated focus in the area using all available resources.

Officers utilized Crimestat, calls for service, complaints, incoming intelligence, and current crime trends when determining the hotspot area.

Members assigned to this prevention strategy met with area residents within the community. Officers walked the beat and patrolled the area in marked police vehicles looking for any suspicious activity, vehicles or potential problem areas.

Overview - between January 17th, 2012 – February 14th, 2012

As a result:

- 96 individuals were arrested and
- 163 Provincial Offence Notices were issued

These proactive initiatives have led to a number of arrests for strong-arm robberies, drug offences, assaults and breaches of court orders.

Division 11 members are committed to reducing crime and will continue to work to provide a safer community for everyone. The Winnipeg Police Service asks everyone in the downtown area to be vigilant, report any crime that they observe, and assist police in this mutual endeavour.

Homicide Investigation Arrest - Update :: C12-27221

As previously released, on February 14th, 2012, at approximately 1:40 a.m. Winnipeg Police Service Members were dispatched to the 1400 block of St. Matthews Avenue regarding an assault incident.

Upon arrival, officers located two injured adult males. A 20 year old male was transported to the hospital in stable condition suffering from injuries to his upper body. An 18 year old male was transported to the hospital in critical condition where he later succumbed to his injuries.

The victim has been identified as Wahbishkanacot MANDAMIN, 18 years.

Due to the ongoing investigation by members of the Homicide Unit, arrest warrants have been issued for two male suspects.

On February 16, 2012, at approximately 10:00 a.m., a 17 year old male turned himself in at the Public Safety Building regarding the outstanding warrant. He was arrested and charged with: 2nd Degree Murder, Aggravated Assault, and Assault with a Weapon. He has been detained.

A warrant for Manslaughter remains outstanding for **Raymond Gerald BAKER, 19 years.**

BAKER is described as: **Aboriginal, 5'11" tall, fair complexion, brown hair and eyes, thin build and possible goatee**

Anyone with information regarding BAKER's whereabouts is asked to contact police immediately or CrimeStoppers at 204-786-TIPS (8477).

Sexual Assault Investigation Arrest :: R12-14098

As previously released, on February 7, 2012, members of the Winnipeg Police Service received the report of a sexual assault which occurred in the area of the 1500 block of Pembina Highway involving a 21 year old female victim.

The victim indicated that she was travelling on a city bus northbound on Pembina Highway when an unknown male sat beside her. It was at this time the male suspect proceeded to touch the victim's leg. As a result, the female exited the bus near Crescent Drive and Pembina Highway. The male suspect also exited the bus and began following the victim. The suspect kept pace with the victim and subsequently touched her on the lower body. The victim proceeded indoors and the suspect stopped following her.

The investigation continued by members of the District 6 Crime Unit and images of the suspect were released publicly.

On February 16, 2012, a 30 year old male turned himself in at the Public Safety Building where he was placed under arrest. He is facing a charge of: Sexual Assault and released on a Promise to Appear.

Residential Robbery :: C12-29131

On February 16, 2012, at approximately 4:00 a.m., members of the Winnipeg Police Service responded to a residence located in the 800 block of Brewster Street regarding a residential robbery.

At this early stage of the investigation, officers have learned that two male suspects entered the home and confronted a 23 year old male and 24 year old female.

The male victim was assaulted to the upper body and treated for non-life threatening injuries.

Several electronic items were stolen by the suspects.

The investigation is continuing by members of the Major Crimes Unit.

Financial Robbery Arrest :: C12-27482

On February 14, 2012, at approximately 2:40 p.m., officers responded to a financial institution regarding a robbery incident involving an armed male suspect.

A teller was confronted by the suspect who indicated that he was armed. It was at this time the suspect jumped over the counter and obtained an undisclosed amount of cash before fleeing the area. No was injured as a result of the incident.

Due to the investigative efforts of uniform members and members of the Major Crimes Unit, on February 16, 2012, **Armand James DUBOIS, 36 years** was located in the 300 block of Hargrave Street and arrested.

The majority of the stolen funds were recovered by officers.

He has been charged with: Robbery with a Weapon and detained.

Missing Person - Angelica GODIN :: R12-16883

The Winnipeg Police Service is requesting the public's assistance in locating a 15 year old female, **Angelica GODIN**.

GODIN was last seen on February 15, 2012 at approximately 8:30 p.m. in the North end area of Winnipeg.

The Winnipeg Police Service considers GODIN to be a child in need of protection as she is at high risk of being exploited or victimized and investigators are concerned for her well-being.

GODIN is described as **Aboriginal, 5'3, 115 lbs, long brown hair and brown eyes. She was last seen wearing a black hoody, black sweat pants, and black shoes.**

Anyone with information regarding GODIN'S whereabouts is asked to contact the Winnipeg Police Service Missing Persons Unit at 204-986-6250.

Lawful Access - Bill C-30

The Winnipeg Police Service would like to acknowledge formal support for Bill C-30. These legislative improvements surrounding electronic communication will provide police with the necessary tools to more effectively investigate serious crime involving electronic devices and electronic mediums, such as the internet.

Organized crime, sexual predators, gangs and identity thieves are using these mediums to commit serious crime in our country. Canada's legislation has not kept pace with technology, and the purpose of this legislation is to modernize tools used by law enforcement and provide for the preservation of data and information.

Bill C-30 places oversight and reporting provisions on police to safeguard citizen's privacy and defines processes for police to investigate these challenging crimes.

This new law is not about giving police new powers, but rather to update laws to reflect new technologies.

Missing Person - Howard KIPLING :: R12-16850 - Located

The Winnipeg Police Service is requesting the public's assistance in locating a 61 year old male, **Howard KIPLING**.

KIPLING was last seen on Saturday, February 11, 2012, in the Lord Selkirk Area of Winnipeg.

KIPLING is described as: **Aboriginal, 6'0" tall and weighs approximately 170lbs. He has short black wavy hair, brown eyes and wears black framed glasses. KIPLING was last seen wearing a black jacket and black boots.**

Investigators are concerned for KIPLING's wellbeing.

Anyone with information regarding KIPLING's whereabouts is asked to contact the Winnipeg Police Service 204-986-6222 or the Missing Persons Unit at 204-986-6250.

Missing Person - Maurice LACHANCE :: C12-28475 - Located

The Winnipeg Police Service is requesting the public's assistance in locating a 52 year old male, **Maurice LACHANCE**.

LACHANCE was last heard from Thursday, February 16, 2012. Investigators believe LACHANCE may be travelling in the Interlake Region along Highway #6 in a pickup truck.

LACHANCE is described as **Caucasian, 5'11", approximately 180 lbs, medium length brown wavy hair, blue eyes and a thick brown moustache.**

Investigators are concerned for LACHANCE's wellbeing.

Anyone with information regarding LACHANCE's whereabouts is asked to contact the Winnipeg Police Service 204-986-6222 or the Missing Persons Unit at 204-986-6250.

For Further Information Contact Either:

Cst. Jason Michalyshen
Public Information Officer

Cst. Natalie Aitken
Public Information Officer

Office: 204-986-3061
Fax: 204-986-7992
E-mail: WPS-PIO@winnipeg.ca

Last update: February 22, 2012

* Top of Page

The Lowell Green Show

580 CFRA NEWS TALK RADIO


CFRA's Getaway...to Wash


Ottawa's Only Live Local


Steve Madely


Madely's Top 5 Stories


Newsletters

Sign up for all 3 Click here

Oct 03, 2013 **Ottawa**

16°C 3-day Forecast

Ottawa & Regional News

Woman dies in Gatineau fire
University of Ottawa among top 200 world ...
Man acquitted of possessing sawed-off sh ...
Ministry of Health issues warning about ...
Man in custody after Centretown stabbing ...
Councillors support distracted driving d ...
Body found in Casselman
Driver hurt in 417 rollover
Brockville Police say VIA train had to a ...
OC Transpo driver Dave Woodard laid to r ...
Man hit by OC Transpo bus near Laurier S ...
Man wanted in convenience store robberie ...
Ten-bed hospice for Kanata closer to rea ...
War of 1812 veterans memorialized in tow ...
Man charged after D. Roy Kennedy inciden ...
SIU releases initial details surrounding ...
Fire guts abandoned home on Arthur Stree ...
Man killed in downtown crash
Municipal campaign donation rebate progr ...
15-year-old boy charged with threatening ...

More Ottawa & Regional News

Canada & World News

Another beef recall is under way
New leak in Fukushima power plant (1)
Canadians jailed in Egypt end hunger str ...
FBI shuts down drug trafficking website
Gas plant report due next week

More Canada & World News

Business News

Bank of Canada lowers economic growth pr ...
Defined Benefit Pension Plans Healthier
Analysts suggest Blackberry deal could b ...
32 SNC-Lavalin employees admit to ethica ...
Video game maker to expand Quebec operat ...

More Business News

Facebook


Our next 580 CFRA Getaway brings you from one Capital to another. You'll experience art, culture, shopping and even some politics ... in Washington DC!

Read More

Win passes to the premiere screening of The Right Kind of

Canada's Chief Justice wants gender parity on the Supreme Court. Although she stops short of criticizing PM Harper's choice of a male (Justice Marc Nadon), to fill a vacant Que. seat, Justice Beverley McLachlin says the court should be representative of society & noted women now take up more that 50% of law school places. The current makeup after Nadon's appointment is 6 men, 3 women. Do you agree with the Chief Justice?

Yes

No

Vote

Wrong on Wednesday, October 9th at 7.30pm at SilverCity Gloucester.

Read More

More Contests

The Lowell Green Show

The file you have attempted to download is a restricted file type. Please contact IT Client Services at (613) 991-7053 for assistance.

Le ficher que vous avez essayé de télécharger est un fichier réservé. Veuillez communiquer avec les Services de la TI, au 613-991-7053, pour obtenir de l'aide

502 Proxy Error. The ISA Server denied the specified Uniform Resource Locator (URL). (12202)

Twitter

Our updated story - woman dies in early morning Gatineau apartment fire. http://t.co/z1TzZksTuR
12:19:53 PM Oct 3, 2013

Gatineau police say a 58 y/o woman has died following a fire at an apartment block this morning
11:59:23 AM Oct 3, 2013

Madely's Morning Minute - Oct. 03
http://t.co/eTCRVzJVGy
11:43:36 AM Oct 3, 2013

At least 94 dead after migrant boat sinks off Italian island coast. 141 have been saved, but there may have been 500+ on board
11:40:47 AM Oct 3, 2013

Quick Links

Home

BedfordBeacon.com provides local news and information about Bedford, Nova Scotia, Canada.

Partner Sites

- MyScores.ca
- Haliwax.com

Slideshow

Community Directory

- Police and Fire
- Churches
- Medical Services
- Government Reps
- City Services
- Bedford Schools
- Bedford Library
- Community Centres
- Bedford Parks
- Minor Sports
- Welcome Wagon
- Bedford Community Council

Halifax News

- Halifax shipyard gets government financial aide package for navy ships
- Bail denied for Halifax navy officer accused in rare case of espionage
- OrKidstra performers 'take in their stride'
- Neptune to mark 50th season with a party, and you're invited
- 'Tough decisions' ahead for CanJet flight attendants

National News

- Hockey mom's spat with league leads to ban of 7-year-old son
- Is Quebec more Catholic than it likes to think?
- 90-year-old gets apology for 2 a.m. hospital discharge
- Jacques Parizeau, former PQ premier, slams charter of values
- George Parros fight injury in season opener renews debate

International News

- Dozens die in Italy boat sinking
- IMF says US must solve debt crisis
- Worker error causes Fukushima leak
- Madagascar mob kills two Europeans

HRP supports CACP's position on Lawful Access

This post was written by Bedford Beacon Editor on February 21, 2012
Posted Under: News and Information

Earlier today, the Canadian Association of Chiefs of Police (CACP) issued a news release about lawful access (see below).

Chief Frank Beazley of Halifax Regional Police supports the position of the CACP: "I don't believe that citizens should be concerned about Bill C-30 as it's designed to modernize the existing legislation surrounding police access to communication which is already permitted by law and at the same time introduce and tighten oversight processes with respect to these powers. I'd ask citizens who do have concerns to become better informed about the issue of lawful access by visiting www.cacp.ca and considering the public safety perspective."

News Release:

CACP Appeals to Canadians – The Lens of Law Enforcement

"Why we are asking for Lawful Access"

OTTAWA, ON – The Canadian Association of Chiefs of Police (CACP) is asking Canadians to consider the views of law enforcement as they debate what we refer to as ' lawful access', or Bill C-30 – *"An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts."*

President of the CACP, Chief Dale McFee: "The CACP has endorsed lawful access legislation since it was first introduced by government in 2002. Canadians more than understand the exponential growth in technology which has occurred over the last few decades. Yet, law enforcement is being asked to protect the communities we serve based on legislation introduced in 1975 – the days of the rotary phone."

The Global Internet, cellular phones and social media have been widely adopted and enjoyed by Canadians, young and old. Many of us have been affected by computer viruses, spam and increasingly, bank or credit card fraud. These new medias are also being used as a safe haven for serious criminal activity –

- Plane crashes after Lagos take-off

identity theft, child and sexual exploitation, gangs, organized crime and national security threats.

"This is a huge challenge facing law enforcement agencies. We collectively need every reasonable tool to prevent such activity from happening in the first place or to investigate and lay charges when it does. We also need the privacy safeguards to ensure we're accountable in the use of these tools and Bill C-30 provides just that" states OPP Commissioner Chris Lewis."

"The debate – balancing community safety and privacy rights – is a debate which must occur and we are very mindful and respectful of the views of all Canadians. The CACP, however, is disappointed in the amount of misinformation and rhetoric that is clouding an important discussion on this issue. It stems from appealing to the greatest fears of Canadians and suggesting that law enforcement may misuse such legislation. It has been propagated that law enforcement could freely monitor the 'surfing habits of Canadians' and do so without a warrant. "Nothing could be farther from the truth" states Vancouver D/Chief Warren Lemcke, who is also Chair of the CACP Law Amendments Committee.

Obtaining content or monitoring (tracking) communication requires a warrant and this condition remains with C-30. Basic subscriber information (BSI) is an on-going challenge for law enforcement to obtain. In some cases ISP's provide the information, others will not, or often there are lengthy delays. The RCMP's National Child Exploitation Centre states that "in 2010, the average response time for these requests was 12 days." During this time, victims continue to be victimized.

In its report Every Image, Every Child – Internet-Facilitated Child Sexual Abuse in Canada the Office of the Federal Ombudsman for Victims of Crime outlines the very serious issues faced by law enforcement. Canada's Federal Ombudsman for Victims of Crime, Sue O'Sullivan, further underlined the importance of the need for lawful access to Parliament 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)*:

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.

One example that demonstrates the need for this type of information (further examples are provided in the attached correspondence):

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.

The CACP believes that Bill C-30 provides greater oversight to obtain BSI than within the current environment. Today, obtaining basic subscriber information is completely ad hoc and uncontrolled. There is no certainty that basic information can be provided in a timely and consistent manner to law enforcement for investigative purposes.

"Under this new lawful access legislation, strict procedures for recording, reporting and auditing of all requests to obtain BSI are put in place. This information is documented and provided to senior Public Safety officials throughout Canada, including Privacy Commissioners. Those within law enforcement who can obtain BSI information is strictly limited. There is actually significantly more oversight with this legislation than what exists today" Chief McFee reaffirms.

To promote balanced discussion on this issue, the Canadian Association of Chiefs of Police have prepared a document entitled "Simplifying Lawful Access – Bill C-30." It is available on the CACP website (www.cacp.ca). The document compares today's environment versus that proposed under the new legislation, provides answers to 'frequently asked questions' and a series of Case Studies describing the utility of BSI to law enforcement (when it works and when it does not).

Our hope is that Members of Parliament, the media and Canadians as a whole will take the time to view the importance of this legislation through the lens of law enforcement.

The Canadian Association of Chiefs of Police (CACP) 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.

Share this:

Comments are closed.

Next Post: CP Allen student faces drug charges
Previose Post: BRA meeting this evening

Latest Posts

- Our final post…
- A winning team once again!
- Police urge motorists to drive with caution
- RCMP: use caution when approaching bus stops
- These boys are ready for some football
- Bedford man an avid participant in Parkinson SuperWalk
- Holy mackerel!
- Councillor Tim Outhit's Summer 2012 newsletter
- Friday last day for weekly green cart collection
- M&M Meat Shops inspires traditional family mealtimes

Categories

- News and Information
- Sports and Recreation
- Arts and Entertainment
- Photo of the Day Archive

Archives

- September 2012
- August 2012
- June 2012
- May 2012
- April 2012
- March 2012
- February 2012
- January 2012
- December 2011
- November 2011
- October 2011
- September 2011
- August 2011
- July 2011
- June 2011
- May 2011
- April 2011
- March 2011
- February 2011
- January 2011
- December 2010
- November 2010
- October 2010
- September 2010
- August 2010
- July 2010
- June 2010
- May 2010
- April 2010
- March 2010
- February 2010
- January 2010
- December 2009
- November 2009

- October 2009
- September 2009
- August 2009
- July 2009
- June 2009
- May 2009
- April 2009
- March 2009
- February 2009
- January 2009
- December 2008
- November 2008
- October 2008
- September 2008
- August 2008

Subscribe to Feeds

- RSS FEEDS
- Google
- netvibes
- Bloglines
- MY YAHOO!

Search for:

Search

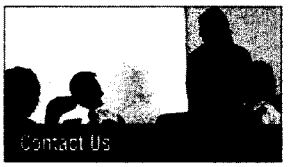
Email Alerts

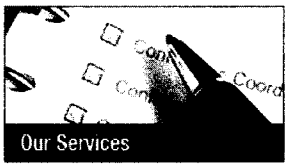
Get email alerts about such things as school cancellations, election results, severe weather and police bulletins.

Email:

- Subscribe
- Unsubscribe

Submit





Conference Quick Search

For general searches use Quick search to select the year and/or month. For a more detailed search click on the Advanced Search

Year Month

Get Results!

Advanced Search

Subscribe to the RSS feed

Follow us on Twitter

Conferences

PRESS RELEASE: FEDERAL/PROVINCIAL/TERRITORIAL MINISTERS DISCUSS KEY JUSTICE AND PUBLIC SAFETY ISSUES FACING CANADIANS

CHARLOTTETOWN, January 26, 2012 – Federal, provincial and territorial (FPT) ministers responsible for justice and public safety concluded their meeting today, after in-depth discussions on key justice and public safety issues currently facing Canadians.

The meeting was co-chaired by the Minister of Justice and Attorney General of Canada, Rob Nicholson, P.C., Q.C., the Minister of Public Safety, Vic Toews, P.C., Q.C., and the Minister of Environment, Labour and Justice and Attorney General of Prince Edward Island, Janice Sherry.

Violence Against Aboriginal Women and Girls
In July 2011 at a meeting of the Council of the Federation, provincial and territorial ministers were asked to consider the root causes of violence against Aboriginal women and girls. Ministers discussed the ongoing work to address the serious issue of violence against Aboriginal women and girls, and invited the federal government to be part of this work and further discussed linkages with other sectors. They agreed to continue to collaborate and develop a common approach.

Missing Women Working Group Final Report
Ministers recognized the progress in examining issues related to the serious concerns surrounding murdered and missing women. They supported the release of the Missing Women Working Group's final report and noted that some recommendations have already been implemented. Ministers asked the working group to bring forward an implementation plan and reiterated their commitment to continue to coordinate their efforts on this important issue. The report is available at www.scics.gc.ca.

Child Pornography and Investigative Complexities
All ministers agreed on the need to enhance and modernize the investigative capability of law enforcement. This is particularly important when dealing with online child exploitation offences and child pornography cases. Provincial and territorial ministers urged the federal government to move forward on enacting previously introduced legislation, specifically former Bill C-52 *(Investigating and Preventing Criminal Electronic Communications Act)*, former Bill C-51 (*Investigative Powers for the 21st Century Act)* and former Bill C-50 (*Improving Access to Investigative Tools for Serious Crimes Act)*. The federal government was also asked to consider increasing the current 21 day data preservation periods for foreign requests to at least 90 days to help law enforcement deal with complex child pornography cases. The federal government welcomed the support of provinces and territories and noted its intention to reintroduce the bills soon.

Proposed Amendments to the *Criminal Code*
Ministers discussed amending the *Criminal Code* to address issues such as home invasion, car-jacking, and the unlawful use of body armour or fortified vehicles or buildings and mandatory minimum penalties for pre-meditated knife crimes. One jurisdiction raised concerns about mandatory minimum penalties. Ministers agreed that these matters should be referred to senior officials for their consideration and to provide recommendations back to Ministers. Ministers also received a status report on the ongoing work to update the corruption provisions of the *Criminal Code*.

Mental Health and Justice
Ministers acknowledged that mental health issues present significant challenges for the justice system. Ministers highlighted the success of the May 2011 Mental Health and Justice Symposium in Alberta and discussed the Symposium's recommendations. Ministers asked senior officials to further engage their health and social service counterparts in reviewing the recommendations and developing a workplan with the view of more effectively managing this at-risk population.

Drug Treatment Court
Ministers acknowledged the value and importance of coordinated federal, provincial and territorial funding for drug treatment courts as an alternative model for drug addicted offenders within the criminal justice system. Provincial and territorial ministers urged continued federal funding for the existing drug treatment courts. There was also a request to consider expanding the program for such courts and other therapeutic courts. The federal Minister of Justice indicated that he would take these concerns under advisement.

Fetal Alcohol Spectrum Disorder (FASD) and Access to Justice
Ministers agreed that the response of the justice system to those with FASD continues to be a priority and noted the importance of prevention. Ministers directed FPT officials to continue to work together to explore how to best respond to individuals with FASD.

Northern and Remote Justice
Ministers noted the challenges and opportunities faced by the territories and most provinces related to the administration of justice in northern and remote regions. Ministers directed senior officials to continue their joint efforts in raising the profile and responding to these issues. A conference on northern and remote policing will be held in the fall of 2012 in the Yukon.

National Police Services
Ministers discussed the importance of the RCMP National Police Services which provides specialized investigational support services to more than 500 law enforcement and criminal justice agencies across Canada. Ministers endorsed the establishment of a National Police Services Advisory Committee that will include representation from the provinces, territories and the RCMP. The Advisory Committee will be co-chaired by a provincial or territorial representative.

Economics of Policing
Ministers discussed the challenges of the escalating costs of policing and the work underway to improve efficiency and effectiveness. Ministers supported enhanced information sharing among jurisdictions on best practices and stressed the importance of collaboration among all law enforcement partners to fight the root causes of crime. All ministers expressed support for a National Summit on the Economics of Policing in fall 2012.

Police Officers Recruitment Fund
Ministers discussed the effectiveness of the Police Officers Recruitment Fund, which has assisted provinces and territories in increasing police resources for community safety and combatting organized crime. Provincial and territorial ministers expressed their desire for the fund to be extended past March 31, 2013 on a permanent basis. The federal Minister of Public Safety indicated that the government had delivered on its five year funding commitment but agreed to bring this forward for government consideration.

First Nations Policing Program
Ministers discussed the First Nations Policing Program, recognizing its importance in addressing challenges to public safety in First Nation and Inuit communities. Provincial and territorial ministers underlined the importance and effectiveness of the Program. They emphasized the need for sustainability and for expanding the program including to the North. The federal government acknowledged the importance of this program in Aboriginal communities and agreed to work with all jurisdictions on this matter recognizing the current environment of fiscal restraint.

RCMP Referral to Victims Services
All ministers agreed on the importance of providing victims of crime with information and quick access to victim services. Provincial and territorial ministers asked the federal government to consider regulatory reform to ensure that the RCMP can share victim information with provincial and territorial victim services. Ministers look forward to receiving recommendations from senior officials on a long-term sustainable solution for the issue.

Federal Legislative Reform Items
Ministers discussed the implementation of Bill C-10 and acknowledged that many of the reforms in Bill C-10 have been the subject of previous discussions over the past several years, in which several jurisdictions have expressed support for these reforms. One jurisdiction expressed its concern with two provisions concerning youth justice and some provinces and territories voiced the importance of prevention in conjunction with enforcement and sentencing measures. In addition, provincial and territorial ministers noted that their concerns focus primarily on the elements of C-10 which may result in additional pressures on the justice system, including the need for increased funding. The provinces and territories presented a resolution in regards to collaboration and consultation. Provincial and territorial ministers expressed concerns with respect to notification of proclamation dates and requested that the federal government improve their protocols for notifying the provinces and territories in a timely manner of the coming into force of legislation. Federal ministers agreed on the need for continued collaborative dialogue in managing the shared FPT responsibility in criminal justice. Federal Ministers stated that the views of the provinces and territories will be considered regarding the coming into force of amendments included in Bill C-10 and that a staggered implementation of amendments to the Criminal Code, Youth Criminal Justice Act and the Controlled Drugs and Substances Act within a reasonable time will facilitate preparation for implementation for all jurisdictions.

Long-Gun Registry Data
Quebec reiterated its previous request to transfer to the province all non-restricted firearms registry records related to its residents. Support for this request was expressed by some jurisdictions.

Legal Aid
Ministers affirmed their commitment to a responsive, fair, efficient and accessible justice system which includes access to legal aid and referenced the common statement of principles approved in October 2010. Provincial and territorial ministers asked the federal Minister of Justice for continued and enhanced federal funding support for criminal legal aid to address the continued pressures faced by all legal aid programs. They asked for early confirmation of the level of federal funding given that existing agreements expire at the end of March 2012. Provincial and territorial ministers also noted the need for renewed and enhanced funding for immigration and refugee legal aid for those jurisdictions offering such services.

Trafficking in Persons
The Government of Canada presented an overview of its draft *National Action Plan to Combat Trafficking in Persons* and invited input from the Provinces and Territories. The federal government will regularly report on its progress.

Family Property and Bankruptcy and the Divorce Law
Provincial and territorial ministers identified the need to amend the *Bankruptcy and Insolvency Act* to ensure persons who declare bankruptcy are not relieved of obligations under provincial marital property legislation. The Federal Justice Minister agreed to raise the issue with his federal colleagues. The federal Minister of Justice acknowledged a request for amendments to section 25.1 of the *Divorce Act* and took the request under advisement.

Justice System Reform, Prevention and Rehabilitation

In discussing priorities for their work moving forward, Ministers identified the need to collaborate in achieving justice system reform. Ministers acknowledged the importance of substantive law reform, but also acknowledged the need to identify process reforms that will improve efficiency and increase system capacity. There was also discussion of increasing court capacity by moving non-criminal matters out of the courts, to increase capacity of the system to address more serious offences. Ministers also discussed the importance of prevention as an effective means to reduce crime and thus victimization.

Ministers requested senior officials to establish two committees – one on prevention and rehabilitation and the other on access to justice and justice system reform.

Ministers also discussed the Canada–U.S. Shared Vision for Perimeter Security and Economic Competitiveness Action Plan, countering violent extremism and random breath testing.

–30–

Julie Di Mambro
Press Secretary
Office of the Minister of Justice
613-992-4621

Julie Carmichael
Press Secretary
Office of the Minister of Public Safety
613-991-2865

Media Relations Office
Department of Justice
613-957-4207

Media Relations Office
Public Safety Canada
613-991-0657

DATE MODIFIED: 3-10-2013

IMPORTANT NOTICES

Resolutions Adopted at the 106th Annual Conference

August, 2011
Windsor, Ontario

CANADIAN ASSOCIATION OF CHIEFS OF POLICE
Leading progressive change in policing

Unit 100 – 300 Terry Fox Drive, Kanata Ontario K2K 0E3
p: 613-595-1101 f: 613-383-0372
e: cacp@cacp.ca w: www.cacp.ca

Table of Contents

Resolution #01 - 2011

REINTRODUCE LAWFUL ACCESS LEGISLATION TO REDUCE LAWFUL ACCESS AND ELECTRONIC SURVEILLANCE DEFICIENCIES AND OBSOLESCENCE

Submitted by the Law Amendments Committee

WHEREAS current *Criminal Code* provisions in respect to police powers to conduct judicially authorized electronic interceptions and seizures are outdated and not in touch with modern realities, and;

WHEREAS modernization of these legislative provisions is urgently required to reflect the significant advancements in communications technologies, and;

WHEREAS there are no requirements for new telecommunications technologies to be intercept capable, and;

WHEREAS the current legislative scheme has resulted in intercept safe havens.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police urge the Federal Government to pass legislation to amend the *Criminal Code* to require new telecommunications technologies to be intercept capable, to prevent intercept safe havens and to modernize electronic intercept provisions.

Resolution #01 - 2011

REINTRODUCE LAWFUL ACCESS LEGISLATION TO REDUCE LAWFUL ACCESS AND ELECTRONIC SURVEILLANCE DEFICIENCIES AND OBSOLESCENCE

Submitted by the Law Amendments Committee

Commentary:

Repeated attempts to introduce lawful access legislation have received government and all party support, however, the legislation has encountered the conclusion of parliamentary sessions prior to third reading.

Canada's obsolete legislative scheme was implemented during the days of the rotary dial telephone. Modernization of current legislative provisions is urgently required to reflect significant advancements in communications technologies – such as emails, encryption, and text based messaging. These 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.

Unlike previous telephony data and technology, where a phone was hardwired into a specific location and communicated to another phone hardwired at the receiving end, new technologies operate much differently. Technology is mobile, operating on wireless frequencies routed through any number of internet service providers worldwide. Intercept is much more complex and requires advanced technologies and updated legislation to compete with criminals. Currently a number of new telecommunications technologies cannot be intercepted, allowing criminals a fail safe way to conduct business without the prying eyes of police. Other G-8 countries around the world require new telecommunications technologies to be 'intercept capable'.

Without modernization, the current legislation challenges police investigative techniques and compromises public safety. Urgent amendments are required to allow the police to lawfully and effectively investigate serious offences; particularly those committed by organized crime groups and gangs.

Resolution #01 - 2011

REINTRODUCE LAWFUL ACCESS LEGISLATION TO REDUCE LAWFUL ACCESS AND ELECTRONIC SURVEILLANCE DEFICIENCIES AND OBSOLESCENCE

Submitted by the Law Amendments Committee

Media Lines:

- The current legislation that is in effect relating to Lawful Access was implemented during the days of the rotary phone. With the continuing advances being made to electronic technology, this legislation is now obsolete and it compromises public safety by challenging police investigative techniques.

- Urgent amendments are required to allow the police to lawfully and effectively investigate serious offences that are being perpetrated using new and advanced communication technologies; particularly those offences committed by organized crime groups and gangs.

- Prior to parliament being prorogued, new Lawful Access legislation was introduced and it received all party support through its first and second readings. With parliament back in session, Bills C-46 and C-47 should be reintroduced in order to proceed to a third and final reading.

- These two Bills will provide the police with the tools that are necessary to deal with new and emerging crime trends associated with modern communication technology.

Resolution #02 - 2011

INTRODUCE ELECTRONIC COUNTERMEASURES LEGISLATION

Submitted by the Law Amendments Committee

WHEREAS Electronic Countermeasures (ECM) are available for purchase by the general public on the open market, and;

WHEREAS the Federal *Radiocommunication Act* does not provide clear guidelines for the possession and use (application) of Electronic Countermeasures, or clear prohibitions which will allow for an effective law enforcement response, and;

WHEREAS it has been proven that electronic countermeasures are effective tools, now being used by organized crime, to disrupt police communication systems including computer aided dispatch, police radios, and cell phones, and;

WHEREAS officer and public safety is compromised when law enforcement officials are left without communications when dealing with individuals possessing this technology.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police urge the Federal Government of Canada to introduce legislation pertaining to Electronic Countermeasures that will restrict the possession and use (or application) of this technology under the *Criminal Code* and the *Radiocommunication Act*. This legislation should give law enforcement officials the usual powers of arrest and detention, with the accompanying provisions for the search and seizure of this technology, when electronic devices are being used contrary to law.

Resolution #02 - 2011

INTRODUCE ELECTRONIC COUNTERMEASURES LEGISLATION

Submitted by the Law Amendments Committee

Commentary:

Electronic Countermeasure (ECM) devices, or jammers, have been in existence for a number of years. They were originally employed by the military to interfere with hostile communications and to mask their own activities from electronic surveillance. ECM devices have evolved from an unsophisticated "brute force" wide band application to either blocking discreet bands of the RF spectrum or blocking some of the spectrum while allowing certain frequencies to operate without interference. These devices are now available on the open market. Some are sophisticated in their design and come in a variety of shapes and sizes, from small units that are the size of a cigarette lighter inserts, to larger, more powerful vehicular mounted unites. They are advertised openly by companies inside Canada. These devices can prevent a police officer from communicating with their dispatch or other police officers.

These devices and the purpose for which they are created are inherently harmful and lend themselves to use by organized crime and other elements in furtherance of criminal activity. The danger they pose to the life and safety of all public safety officers is self evident. Absent an exemption or licensing scheme authorizing use by government agencies and public safety designates, the possession, importation, sale and manufacture of these devices must be made illegal in Canada. The regulation of these devices belongs in the *Criminal Code* and they should be dealt with in the same manner as other prohibited devices.

Resolution #02 - 2011

INTRODUCE ELECTRONIC COUNTERMEASURES LEGISLATION

Submitted by the Law Amendments Committee

Media Lines:

- Electronic Countermeasures (ECM) are devices that were originally designed and employed by the military to interfere with electronic communications.
- These devices are now available on the open market and they are being advertised by companies inside of Canada.
- It has been proven that these devices are now being used by organized crime groups to disrupt police communication systems.
- When law enforcement officials are left without communications, officer and public safety is compromised.
- The Canadian Association of Chiefs of Police strongly believe that these devices should be regulated by the *Criminal Code* in the same manner as other prohibited devices.

Resolution #03 - 2011

PROVIDE 9-1-1 CELL PHONE CALL CUSTOMER NAME AND ADDRESS

Submitted by the Law Amendments Committee

WHEREAS we live in a society that now relies heavily on mobile communication, and;

WHEREAS there should be no difference in the level of safety available pursuant to a 9-1-1 call that is made from a landline and a call that is made from a cell phone, and;

WHEREAS there is a gap in the Canadian Radio-Television and Telecommunication Commission's policy that only requires the release of the number and not the name and address associated with a cell phone that an emergency call is originating from, and;

WHEREAS there are unnecessary delays occurring before the police can be dispatched to an emergency call made from a cell phone because of the current back grounding and risk assessment steps that are required on 9-1-1 calls from cell phones prior to the identification of the associated address and public safety is compromised when these delays occur.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police urge the Federal Government of Canada to move forward with legislation that would require Wireless Service Providers to immediately provide Public Safety Answering Points with subscriber name and address on all 9-1-1 calls, and;

BE IT FURTHER RESOLVED that the Canadian Association of Chiefs of Police urge the Canadian Radio-television and Telecommunication Commission to take immediate steps to amend Telecom Decision 2009-40 by making it mandatory for Wireless Service Providers to provide subscriber name and address on all 9-1-1 calls from cell phones.

Resolution #03 - 2011

PROVIDE 9-1-1 CELL PHONE CALL CUSTOMER NAME AND ADDRESS

Submitted by the Law Amendments Committee

Commentary:

Currently there is a distinction made between the information that a Public Safety Answering Point (PSAP) receives on a 9-1-1 call that is made from a landline and a 9-1-1 call that is made from a cell phone. Canadian Radio-television and Telecommunication Commission's policy, under Telecom Decision 2009-40, mandates Wireless Service Providers to provide the phone number of a cell phone and, unlike a landline, not also provide the subscriber's name and address associated with the cell phone when an emergency call is placed.

This leads to unnecessary delays in police response. There have been recent incidents of domestic violence that have ended tragically after calls for help were made using cell phones where customer name and address were not readily available. This is unacceptable in a society where individuals calling 9-1-1 do so to receive immediate assistance.

Resolution #03 - 2011

PROVIDE 9-1-1 CELL PHONE CALL CUSTOMER NAME AND ADDRESS

Submitted by the Law Amendments Committee

Media Lines:

- In a society where more and more people are using wireless communications for all of their telephone needs, subscriber name and address information represents an initial 'building block', or starting point, from which the police can proceed with their variously required statutory and common law duties – crime prevention, investigation, maintenance of public safety, and others.

- The safety and security of our communities' demands that appropriate and reliable subscriber information be provided to Public Safety Answering Points in order that they may appropriately assess the risks to members of the public, and to locate them in situations of urgency, when seconds count. The current scheme of only providing the telephone number along with unreliable XY coordinates, thereby imposing additional time consuming steps for the assessment of risk and caller location during emergency 911 calls requires immediate changes to CRTC policy.

- It is with this in mind, that the Canadian Association of Chiefs of Police urges the Canadian Radio-television and Telecommunication Commission to take immediate steps to amend CRTC Telecom Decision 2009-40.

Resolution #04 - 2011

AMENDMENT TO THE *CRIMINAL CODE OF CANADA* AND THE *DNA IDENTIFICATION ACT*

Submitted by the Law Amendments Committee

WHEREAS DNA Analysis is an invaluable tool in the investigation and prosecution of criminal offences, as well as the protection of society and the exoneration of the innocent, and it is in the public interest to have investigations proceed as expeditiously as possible, and;

WHEREAS the system established in the *Criminal Code* requiring a conviction for a primary designated offence and the issuance of a court order before a DNA sample can be collected is administratively cumbersome and results in considerable delay, and;

WHEREAS the court has limited jurisdiction to decline to order a DNA sample on a primary designated offence, and;

WHEREAS the delay between arrest and conviction can be lengthy and the consequent delay in the obtaining of a DNA sample can seriously compromise outstanding investigations.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police urge the Federal Government of Canada to move forward with amendments to the *Criminal Code of Canada* and *DNA Identification Act* to allow for:

- The collection of DNA samples from any person lawfully charged for a primary designated offence, as defined in section 487.04 of the *Criminal Code*, by part (a) of the definition of "primary designated offences"; and,

- The removal of that sample from the DNA Databank should the accused not be convicted of the offence (post appeal periods).

Resolution #04 - 2011

AMENDMENT TO THE *CRIMINAL CODE OF CANADA* AND THE *DNA IDENTIFICATION ACT*

Submitted by the Law Amendments Committee

Commentary:

There is no other forensic identification technique (fingerprints, ballistics, tire tracks and tool marks) that is as effective as DNA in identifying individuals who have committed a crime or in exonerating a person suspected of committing a crime. In section 4 of the *DNA Identification Act*, it is specifically stated that "the protection of society and the administration of justice are well served by the early detection, arrest and conviction of offenders, which can be facilitated by the use of DNA profiles".

In Europe, where England is widely recognized as having one of the most successful approaches to the use of forensic DNA technology, statistics show that with over 2 million DNA profiles loaded into their system there is a 40 percent greater chance of obtaining a match between a crime scene profile and a "criminal justice" (arrestee or suspect) profile.[1]

Currently, an offender's DNA is not checked against the Databank until a conviction is entered and an Order granted for collection of a sample, unlike with fingerprinting where fingerprints are taken at the time of arrest and compared to the fingerprint database. Unsolved cases in the Databank can remain on hold for a considerable amount of time waiting for an offender's DNA to be submitted. In addition, there is often considerable delay between arrest and conviction, this results in an added delay of up to years before cases in the Databank can be properly investigated and the offenders either identified or exonerated. It is important to note that a hit on the Databank only allows the investigation to proceed to the obtaining of a warrant.

Delays in obtaining a sample for comparison to the Databank mean that previous offences committed by the offender remain unsolved until conviction for the new offence. This means that an accused who has committed other crimes will go undetected for years while awaiting trial for his current arrest, leaving victim's without answers and allowing an accused on bail to continue to commit similar offences, undeterred. Should an accused not be convicted, that sample will be removed from the Databank and destroyed. Many accused fail to attend court and many individuals who are required to provide DNA do not do so. Collecting DNA at the time of arrest ensures that a sample is provided.[2]

---

[1] Asplen, Christopher. *The Application of DNA Technology in England and Wales*. Smith Alling Lane. Received by the US Department of Justice January 2004. p.1.

[2] Victims of Violence. (2008). *Research – DNA Databanks*. Retrieved March 8, 2011 from http://www.victimsofviolence.on.ca/rev2/index.php?option=com_content&task=view&id=341&Itemid=31

The offences described in 487.04, "primary designated offences" (a), are the most serious offences in the *Criminal Code* (murder, aggravated sexual assault, kidnapping, robbery, etc.) and the Court "shall" order a DNA sample upon conviction. This is in contrast to other primary designated offences described in section 487.04 "primary designated offences" (a.1) – (d) and "secondary designated offences" described in section 487.04, where the Court has some discretion in ordering a sample upon conviction. The public has a special interest in ensuring swift investigations of these most serious offences.

If the *Criminal Code* is amended to allow for the taking of a sample at the time of arrest for a s.487.04 "primary designated offence"(a), hits on the Databank will be identified much earlier, and investigations will be able to proceed expeditiously. The elimination of delay benefits the administration of justice by ensuring that investigations are conducted when other evidence can still be obtained and witness memories are fresh. In addition, trials are conducted within a reasonable time which allows compliance with the accused's constitutionally protected right.

Resolution #04 - 2011

AMENDMENT TO THE *CRIMINAL CODE OF CANADA* AND THE *DNA IDENTIFICATION ACT*

Submitted by the Law Amendments Committee

Media Lines:

- The use of DNA to identify individuals who have committed a crime, or to exonerate a person suspected of committing a crime, is more effective than any other forensic technique.

- Unlike fingerprints which are taken at the time of arrest and compared to the fingerprint database, DNA is not checked against the national Databank until a conviction is entered and an Order granted for collection of a sample.

- Additionally, many accused fail to attend court and many individuals who are required to provide DNA do not do so. Collecting DNA at the time of arrest ensures that a sample is provided

- This current process causes timely delays in solving cases that are under investigation, as well as other crimes that the suspect may have committed previously. The Paul Bernardo and Russell William cases in Ontario are both perfect examples of this.

- If the *Criminal Code* is amended to allow for the taking of a sample at the time of arrest for a s.487.04 "primary designated offence", hits on the Databank will be identified much earlier, and investigations will be able to proceed expeditiously.

- The public has a right to expect that these investigations will be carried out quickly and effectively, which will also serve to help prevent the commission of future offences by these offenders.

- Ultimately, the elimination of these delays will benefit the administration of justice in Canada.

Resolution #05 - 2011

UNEXECUTED DNA ORDERS

Submitted by the Law Amendments Committee

WHEREAS DNA Analysis is an invaluable tool in the investigation and prosecution of criminal offences, as well as the protection of society and the exoneration of the innocent, and;

WHEREAS the *DNA Identification Act* became law on June 30, 2000, and;

WHEREAS peace officers are responsible for executing DNA Orders issued by the courts "To Have Bodily Substances Taken", and;

WHEREAS there continue to be a number of legislative gaps in the processes related to DNA Orders and there are hundreds of outstanding DNA Orders across the country that have not been executed, potentially posing a serious threat to public safety.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police urge the Federal Government of Canada to move forward with amendments to the *Criminal Code* to provide that:

- DNA Orders are valid until executed; and,
- Unexecuted DNA Orders may be executed anywhere in Canada.

Resolution #05 - 2011

UNEXECUTED DNA ORDERS

Submitted by the Law Amendments Committee

Commentary:

The *DNA Identification Act*, S.C. 1998, as am. 2000, c. 10 ("*DNA Act*") provides a legal framework to regulate the storage and collection of DNA data and the biological samples from which they have been derived. The *DNA Act* provides for the structure and administration of a national DNA data bank. This database is maintained by the Royal Canadian Mounted Police ("RCMP") and is used to assist Canadian law enforcement agencies in the investigation of serious crimes.

The *DNA Act* must be read in conjunction with the *Criminal Code*, R.S.C. 1985, c. C-46 ("*Criminal Code*") provisions dealing with the collection and use of DNA samples. In January 2008, the Criminal Code was amended to expand on the criteria and procedure for collecting the DNA samples.

The *Criminal Code* provisions provide for a provincial court judge to grant an Order for the collection of DNA sample when he or she was satisfied that a designated offence had been committed.

Designated offences are generally serious personal injury offences. The judge has to be satisfied that the issuance of the Order is in the best interests of the administration of justice. Amendments made in January 2008 now provide that a judge may specify in the Order when and where the offender is to attend for the taking of their DNA samples (*Criminal Code*, section 487.051(4)).

Similarly, the amendments now include a provision that allows a warrant be issued for the arrest of any offender who fails to comply with such an Order.

Prior to these amendments, however, hundreds of DNA Orders from across the country had gone unexecuted.

Although not an exhaustive list, on review it would appear that most outstanding DNA Orders went unexecuted for one or more of the following reasons:

1. A non-custodial offender was never turned over to a police officer for DNA sampling;

2. Alternatively, a non-custodial offender was transported to a location to allow a police officer to take a DNA sample, but no officer was available to execute the order;

3. The offender was never served with an "Order to a Person to Have Bodily Substances Taken for Forensic DNA Analysis"; and as a result, the offender left the court without regard to the order;

4. After January 1, 2008, the court did not make an Order in Form 5.041 indicating a specific date, time and place for the offender to attend in order to have his/her DNA sample taken;

5. The custodial offender completed the sentence and was released without submitting a sample of their DNA.

While law enforcement agencies remain in possession of unexecuted Court Orders to obtain DNA samples from the offenders who have committed primary and secondary designated offences (as defined within s. 487.04 of the *Criminal Code*), they cannot execute the Orders without risking breaching section 487.056 of the *Criminal Code* which mandates that DNA samples should be obtained:

> (a) at the place, day and time set out in an order made under subsection 487.051(4) *or as soon as feasible afterwards* or;
>
> (b) in any other case, on the day on which the order authorizing the taking of the samples is made *or as soon as feasible afterwards*. [emphasis added]

Resolution #05 - 2011

UNEXECUTED DNA ORDERS

Submitted by the Law Amendments Committee

Media Lines:

- The *DNA Identification Act* became law on June 30, 2000, and it provides a legal framework for the collection and storage of DNA data and the biological samples from which they have been derived.

- There were a number of legislative gaps in the original processes related to these DNA Orders that were not immediately identified (but have since been rectified).

- As a result of some of those previous legislative gaps, there are hundreds of outstanding DNA Orders across the country that have not been executed, which is a serious public safety concern.

- Delays in obtaining a sample for comparison to the Databank mean that previous offences that may have been committed by the offender will remain unsolved, and future offences may go undetected.

- Statistics in England show that with over 2 million DNA profiles loaded into their database there is a 40 percent greater chance of obtaining a match between a crime scene profile and a "criminal justice" (arrestee or suspect) profile.

- In order to deal with the issue of these outstanding DNA Orders, the Canadian Association of Chiefs of Police would like to urge the Federal Government of Canada to proceed with amendments to the *Criminal Code of Canada* and *DNA Identification Act* to allow the courts, on application, to reissue an outstanding DNA Order which compels an affected person to attend at a specific date, time and place to provide a sample as per their original Order; and, should it be demonstrated that the affected person cannot be located for service of such an Order, legislative amendments should also allow for an application to be made to issue a Canada-wide warrant to briefly detain and take a sample upon locating the affected person.

Resolution #06 - 2011

BUILDING ON FINANCIAL INTELLIGENCE IN ORGANIZED CRIME INVESTIGATIONS THROUGH FINTRAC

Submitted by the Organized Crimes Committee

WHEREAS there is an effort to support the collaborative nature of the Canadian Law enforcement community, and to enhance the coordination of investigations related to Organized Crime as no single agency can effectively combat organized crime independently, and;

WHEREAS the importance of active leadership to ensure effective and efficient integration of operations and intelligence has been identified, and;

WHEREAS it has been recognized that financial advantage is the key goal for all criminal organizations, and that consequently, financial intelligence must be an integral component of all organized crime investigations, and;

WHEREAS the mandate of FINTRAC is to facilitate the detection, prevention and deterrence of money laundering, terrorist activity financing and other threats to the security of Canada through the analysis of information and dissemination of financial intelligence relevant to such investigations, and;

WHEREAS it would be beneficial to Canadian Law Enforcement agencies to maximize the use of financial intelligence provided by FINTRAC in organized crime investigations to increase the cooperation in detecting and combating money laundering and organized crime.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police calls on all Canadian law enforcement agencies to include financial intelligence in their investigations, and share with FINTRAC their Provincial and National enforcement targets.

Resolution #06 - 2011

BUILDING ON FINANCIAL INTELLIGENCE IN ORGANIZED CRIME INVESTIGATIONS THROUGH FINTRAC

Submitted by the Organized Crimes Committee

Commentary:

The Financial Transactions and Reports Analysis Center of Canada (FINTRAC) was created in 2000 with the adoption of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), with a mandate to detect, deter and prevent money laundering and terrorist activity financing. Eleven years later, police and the security and intelligence community view the Centre's tactical and strategic financial intelligence products as integral to investigations, prosecutions, intelligence collection and decision-making.

The Centre fulfills its mandate through the following activities:

- gathering and analyzing information on suspect financial activities;
- ensuring those subject to the PCMLTFA comply with reporting, record keeping and other obligations;
- making case disclosures of financial intelligence to the appropriate law enforcement agency, CSIS or other agencies designated by legislation in support of investigations and prosecutions; and
- enhancing public awareness and understanding of matters related to money laundering.

Drawing on its database of millions of financial transaction records, FINTRAC analysts can trace the proceeds of crime money trail for law enforcement, identifying potential suspects and tracking proceeds of crime movements through money laundering activities. The bulk of the hundreds of cases FINTRAC discloses to law enforcement throughout Canada involve voluntary information requests from police for financial intelligence regarding criminal activities such as drug trafficking, fraud and organized crime. FINTRAC offers a unique resource for police because it can, through analysis of the reports submitted by financial institutions, follow the money trail across the country and in many cases offshore. Sophisticated organized crime rings will often use elaborate schemes and many different financial institutions to hide their profits, making it next to impossible for a single police force to track.

The OCC realizes the importance of financial intelligence in the fight against organized crime. In fact, money laundering is an integral process of criminal organizations' activities. Criminal organizations will use all techniques at their disposal, including key facilitators and the banking systems without limiting themselves to domestic transactions.

Realizing that all this financial information is being gathered through FINTRAC, the OCC acknowledged the benefits for FINTRAC to be kept apprised of the issues faced by Law Enforcement agencies and included FINTRAC in its membership.

The law enforcement community also realized that it has an important role to play in ensuring that intelligence agencies are provided with timely and accurate information. With this in mind, a resolution was introduced by the CISC National Executive Committee in 2009 (2009-05) to ensure that all approved operational plans targeting organized crime must be uploaded on ACIIS at the onset of the investigation. This provided the appropriate level of leadership, and ACIIS is now part of most police organization policies, and the necessary intelligence is therefore made available to the intelligence community.

This proposed resolution is intended to be in that same line. It seeks the CACP leadership and endorsement for financial intelligence to become a component of all organized crime investigations. It also seeks for FINTRAC to be recognized as a key partner and as such, informed of the law enforcement community's enforcement priorities across Canada. This will assist FINTRAC to align its priorities with law enforcement and improve the quality of the disclosure cases being produced.

Resolution #06 - 2011

BUILDING ON FINANCIAL INTELLIGENCE IN ORGANIZED CRIME INVESTIGATIONS THROUGH FINTRAC

Submitted by the Organized Crimes Committee

Media Lines:

- The CACP Organized Crime Committee (OCC) is focused on addressing the needs of the Canadian Law enforcement community in combating organized crime, promotes innovative law enforcement strategies and contributes to public policy and legislative change as a meaningful partner to the safety and security of Canadians and international partners.

- Following the money trail can shed light on criminal activity as money laundering has basically become standard practice among the criminal organizations.

- The OCC sees added-value to the fact that financial intelligence become a component of all organized crime investigations.

- To this end, FINTRAC has to be recognized as a key partner and is made aware of the enforcement priorities across Canada. This will in turn assist FINTRAC to align its priorities with law enforcement and improve the quality of the disclosure cases being produced.

- Created in 2000, FINTRAC is an independent agency with a mandate to assist the detection, deterrence and prevention of money laundering, terrorist financing and other threats to the security of Canada

- FINTRAC is an intelligence agency and our key product is financial intelligence.

- FINTRAC is one of the most automated financial intelligence units in the world, receiving and processing almost all of its financial transaction information electronically.

- FINTRAC has been able to make a contribution to hundreds of investigations each year of organized crime, smuggling, drug trafficking, and fraud.

Resolution #07 - 2011

NATIONAL POLICE SERVICES

Submitted by the CACP Special Subcommittee on National Police Services

WHEREAS the Canadian Association of Chiefs of Police (CACP) remain committed to support of policing in the Federal, provincial, municipal and First Nations realms, and;

WHEREAS the impact of service delivery of National Police Services is essential to the delivery of police services across Canada, and;

WHEREAS the delivery of said service requires an effective and efficient provision of National Police Services, and;

WHEREAS the effective delivery of consistent service and national standards can only be accomplished through a adequately resourced and funded National Police Services, and;

WHEREAS the CACP Special Purpose Subcommittee on National Police Services is mandated to make recommendations regarding service delivery in relation to those services as defined as "National Police Services".

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police recommend that the Federal Government of Canada - represented by Public Safety Canada, adequately resource and appropriately fund the National Police Services, and;

BE IT FURTHER RESOLVED that an NPS Advisory Committee, representing the regions of Canada, be formed to assist with the governance and future direction of NPS.

Resolution #08 - 2011

CANADIAN TRAINING STANDARD FOR CHILD EXPLOITATION INVESTIGATORS

Submitted by the E-Crime Committee

WHEREAS Canadians have connected to the Internet and embraced computer related technologies at one of the highest rates in the world, and;

WHEREAS child exploitation has become an issue of national and international significance that demands the attention of law enforcement agencies and the criminal justice system, and;

WHEREAS to address these demands the Canadian Association of Chiefs of Police created the e-Crime Committee in 2002 with the mandate of this Committee to establish a CACP leadership role in the development of administrative policy and standards for technology-based investigations, the promotion of inter-agency cooperation in the detection and investigation of child exploitation and exploited children abuses, the establishment of training standards and the identification of effective cooperative strategies to combat e-Crime at a local, Provincial, Canadian and International level, and;

WHEREAS the committee has addressed in its Strategic Plan the establishment of a leadership role in the development of administrative policy and standards for technology based investigations, the promotion of inter-agency cooperation in the detection and investigation of computer based crime, and the establishment of training standards, and;

WHEREAS the training for Canadian law enforcement agencies by the e-Crime Committee has revealed that while specific standardized training programs exist, disparities exist amongst Canadian law enforcement agencies in the application and enforcement of standardized training for child exploitation investigators, and;

WHEREAS the investigation of child exploitation by untrained, partially trained or self-trained investigators who do not follow training standards and methodologies creates huge risk for the Canadian law enforcement community which may reduce public confidence in the investigative capability of police agencies, undermine procedural fairness and may serve to bring the administration on justice into disrepute, and;

WHEREAS the Canadian Police College has developed and validated specialized child exploitation training courses that are delivered by the Canadian Police College and available to all accredited law enforcement agencies, and;

WHEREAS the Canadian law enforcement community has accepted the Canadian Police College Technological Crime Learning Institute training courses as the "standard" for child exploitation investigators, and;

WHEREAS the CACP e-Crime Committee has endorsed the Canadian Police College Technological Crime Learning Institute Training Program as the basis for all Canadian law enforcement personnel undertaking child exploitation investigations, and further that the CACP e-Crime Committee recommends that such training be delivered in such a manner as to facilitate learning and qualification in both official languages.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police recognizes the current training at the Canadian Police College for child exploitation investigators, as being an approved agency to provide training in Canadian law enforcement agencies, which recognition does not restrict Canadian Association of Chief of Police member law enforcement agencies from acquiring additional forensic computer training, as would support the investigative function in the furtherance of the common goal, of thorough, comprehensive and impartial e-Crime investigations in the best interests of the Canadian administration of justice, and;

BE IT FURTHER RESOLVED that the Canadian Association of Chiefs of Police urges that all member agencies undertaking child exploitation investigations computer undertake these functions only with personnel who have met, at a minimum, the recommended training standards of the Canadian Police College, Technological Crime Learning Institute or other validated training as it pertains to child exploitation investigations.

Resolution #08 - 2011

CANADIAN TRAINING STANDARD FOR CHILD EXPLOITATION INVESTIGATORS

Submitted by the E-Crime Committee

Commentary:

Since the creation of information technology, digital information or data is used in the everyday lives of all Canadian citizens and businesses. The range of electronic criminal opportunities is extensive and will continue to expand in tandem with technological advances in online communications and access.

The investigation of child exploitation cases by untrained, partially trained or self-trained investigators who do not follow training standards and methodologies can potentially be a huge risk for the Canadian law enforcement community which may reduce public confidence in the investigative capability of police agencies, undermine procedural fairness and may serve to bring the administration on justice into disrepute. In some provincial jurisdictions it is the responsibility of the police organizations to provide services according to their level of classification therefore mandating more duty and accountability. The Canadian Police College provides training courses which are necessary to enable all police organizations to provide such services and therefore must be properly funded and equipped to provide specialized training for child exploitation investigations in both official languages as required.

Resolution #08 - 2011

CANADIAN TRAINING STANDARD FOR CHILD EXPLOITATION INVESTIGATORS

Submitted by the E-Crime Committee

Media Lines:

- Child exploitation crimes have become an issue of national and international significance that demands the attention of law enforcement agencies and the criminal justice system.

- Child exploitation investigations by untrained, partially trained or self-trained investigators who do not follow approved methodologies may potentially create a huge risk for the Canadian law enforcement community.

- Although standardized training programs exist, disparities exist amongst Canadian law enforcement agencies in the application and enforcement of standardized training for child exploitation investigators and covert online investigations.

- It is the recommendation of the CACP that all member agencies undertaking child exploitation investigations, and online covert investigations, undertake these functions only with personnel who have met, at a minimum, the recommended training standards of the Canadian Police College Technological Crime Learning Institute or other validated training.

- The Canadian Police College provides training courses, which are necessary to enable all police organizations that provide such services and therefore must be properly funded and equipped to provide specialized child exploitation training in both official languages as required.

Resolution #09 - 2011

EVOLUTION OF THE CANADIAN LAW ENFORCEMENT STRATEGY TO COMBAT ORGANIZED CRIME (CLES)

Submitted by Director General, Criminal Intelligence Service Canada (CISC) on behalf of the National Executive Committee (NEC)

WHEREAS the Canadian Association of Chiefs of Police (CACP) fully endorse the principles and values of integration and intelligence-led policing, and;

WHEREAS the CACP unanimously provided its support in August 2007 to earlier efforts to develop and implement an integrated, intelligence-led Canadian Law Enforcement Strategy (CLES) to combat organized crime , in which a key component was the use of integrated provincial and national threat assessments for enforcement priority setting at the municipal, provincial and national levels, and resulted in the creation of the Council on Public Safety and its subsequent evolution into the Canadian Integrated Response to Organized Crime (CIROC), and;

WHEREAS the CACP acknowledges there is value in formally recognizing the partnership between the functions of intelligence and operations – currently represented by the existing entities of Criminal Intelligence Service Canada (CISC) and the Canadian Integrated Response to Organized Crime (CIROC) – as a means to further the original spirit of CLES in 2007, and that this partnership should be accountable to a common governance framework to achieve consistent, efficient and effective results, and;

WHEREAS the CACP concurs that the existing CISC governance structure should be leveraged by expanding its current mandate to encompass the governance of the CISC/CIROC partnership, at the national and provincial levels, under the banner of the Canadian Law Enforcement Strategy (CLES) to combat organized crime:

THEREFORE BE IT RESOLVED by the Canadian Association of Chiefs of Police that it fully endorses the modernized CLES, under the governance of the National and Provincial Executive Committees, and demonstrates its support by endorsing the CLES Statement of Commitment, which outlines the expectations of the CLES partnership and the roles and responsibilities of CLES stakeholders.

BE IT FURTHER RESOLVED that the Canadian Association of Chiefs of Police recommends that all CACP members in Canada support the modernized CLES and adopt the roles and responsibilities outlined in the CLES Statement of Commitment, as applicable.

Resolution #09 - 2011

EVOLUTION OF THE CANADIAN LAW ENFORCEMENT STRATEGY TO COMBAT ORGANIZED CRIME (CLES)

Submitted by Director General, Criminal Intelligence Service Canada (CISC) on behalf of the National Executive Committee (NEC)

Commentary:

The Canadian law enforcement community has demonstrated its commitment to combating organized crime through a number of initiatives over the years that are based on integration and collaboration across all jurisdictions to create a safer Canada. Furthermore, organizations such as Criminal Intelligence Service Canada (CISC) and its partnership with the ten provincial criminal intelligence bureaus exist to ensure the production and exchange of information and intelligence and to promote an integrated, intelligence-led approach to law enforcement. This approach emphasizes the importance of collecting and sharing information in order to develop timely intelligence products, which ultimately serve to guide tactical, operational and strategic decisions.

Several years ago, the Canadian law enforcement community committed to an initiative to produce integrated threat assessments intended to inform law enforcement decision-makers. In 2007, the Organized Crime Committee (OCC) of the Canadian Association of Chiefs of Police (CACP) brought forward a resolution to both CISC's National Executive Committee (NEC) and the CACP that introduced the Canadian Law Enforcement Strategy (CLES) to combat organized crime.

The strategy was the first step in establishing a link between intelligence and operations. While it was recognized that the full strategy would develop over time, the initial component was based upon the use of integrated provincial and national threat assessments for enforcement priority setting. The unanimous endorsement to proceed with the strategy's development led to the creation of the Council on Public Safety (CoPS) and subsequently evolved into the Canadian Integrated Response to Organized Crime (CIROC). This national committee is comprised of provincial representatives that exchange information on ongoing investigations and best practices on the enforcement efforts in their respective provinces. At the outset of CLES it was envisioned that in addition to a national committee there would be provincial enforcement steering committees that make enforcement decisions based on integrated threat assessments. The provinces that have established such a committee have recognized the benefits of working collaboratively with their intelligence counterparts. A number of other provinces are at varying stages of implementation.

As CIROC has evolved, so too has its relationship with CACP and CISC. In 2009, the CIROC National Committee sought to realign with CISC's NEC rather than remain with the CACP OCC in recognition that its purpose needs to have a link with the intelligence function. While the relationship and accountability measures were not clearly defined, it was understood that a partnership between CIROC and CISC is critical.

In 2010, an external review of CISC's governance identified a number of recommendations focused on the need to modernize practices, renew partnerships and clarify roles and responsibilities. One recommendation in particular spoke of the need to formalize the relationship between CIROC and the NEC and CISC.

To fully consider the review's recommendations, the CISC NEC established a provisional working group on governance consisting of five regional NEC members (dubbed the "Group of Five"), the DG, CISC and a provincial bureau director. During initial deliberations, the group met with the Co-Chair of the CIROC National Committee to examine the origins of CISC, CIROC and the original intent of CLES. It became clear that there was an opportunity to build upon the progress to date and further CLES by bringing together the two existing entities – CISC (representing the intelligence function) and CIROC (representing the operations function) – under a common governance framework (Appendix 1). Given the existing infrastructure of the CISC NEC and Provincial Executive Committees (PECs) it was further felt that the current governance mandate of the NEC and PECs should be expanded to encompass the CISC/CIROC partnership under the banner of CLES.

It was through this lens that the group developed a new vision statement (Appendix 2) for CLES based on the following key concepts: 1) partnership between the functions of intelligence and operations across all jurisdictions; 2) active and meaningful participation; and, 3) unity of effort through an integrated approach. It was then agreed that a statement of commitment (Appendix 3) was required to complement the CLES vision, clarify the expectations of the CLES partnership and outline the roles and responsibilities of CLES stakeholders (Appendix 4).

It is important to note that the CLES roles and responsibilities are not intended to be prescriptive; rather, they are designed to achieve a balance between the need for consistency to achieve the CLES vision while recognizing that there are regional differences in its application. The common denominator to achieving CLES will be the collective leadership through the governance framework of the NEC, at the national level, and the PECs, at the provincial level. These bodies will provide the necessary leadership in developing and adjusting CLES's vision and strategic direction. Furthermore, they will provide the required leadership to monitor and ensure implementation of resolutions from the NEC. Having senior leaders of the Canadian law enforcement community sign the CLES statement of commitment will bring a new level of clarity to the strategy and affirm a broad base of support for the continued efforts towards achieving the CLES vision.

The group made a presentation to the CISC NEC on May 11, 2011 about the proposed CLES vision, statement of commitment and roles and responsibilities. The outcome was support in principle for the proposal and a motion to commence additional consultation with the PECs and CIROC in advance of resolutions to NEC and CACP to adopt the CLES proposal in August 2011. A number of provinces have already implemented an intelligence and operations partnership under the governance of its PEC, while others are in varying stages of implementation. Given all law enforcement agencies in Canada are stakeholders in CLES, it is essential to inform the CACP membership of the CLES proposal as well as to obtain the membership's endorsement and support to proceed with implementation and execution of CLES across all jurisdictions.

Resolution #09 - 2011

EVOLUTION OF THE CANADIAN LAW ENFORCEMENT STRATEGY TO COMBAT ORGANIZED CRIME (CLES)

Submitted by Director General, Criminal Intelligence Service Canada (CISC) on behalf of the National Executive Committee (NEC)

Media Lines:

- The Canadian law enforcement community has made significant progress since the Canadian Law Enforcement Strategy (CLES) to combat organized crime was introduced by the CACP Organized Crime Committee in 2007.

- As a leader of progressive change in law enforcement, the CACP supports the continuous evolution of the Canadian Law Enforcement Strategy to combat organized crime.

- Two existing law enforcement entities – Criminal Intelligence Service Canada (CISC) and the Canadian Integrated Response to Organized Crime (CIROC) – currently represent the functions of intelligence and operations respectively.

- A common governance framework for the collaborative effort of intelligence and operations has been proposed that would see CISC and CIROC under one banner – the Canadian Enforcement Strategy to combat organized crime.

- A common governance framework would be created by expanding the current mandate of the National Executive Committee of CISC, as well as those of CISC's Provincial Executive Committees, to include linking together the collaborative effort of CIROC and CISC under these governing bodies to achieve consistent, efficient and effective results.

- The proposed governance framework includes:
    - A vision statement;
    - A statement of commitment to adopting the vision and framework to be signed off by members of the law enforcement community;
    - Roles and responsibilities of all stakeholders in the Canadian Law Enforcement Strategy.

- The proposed strategy enhancements aim to strengthen unity of effort across all law enforcement agencies in Canada to achieve an effective and proactive response to organized crime and to threats to public safety in Canada.

For reference only:

Resolution #09-2007
Canadian Law Enforcement Strategy to Combat Organized Crime
Submitted by the Organized Crime Committee

WHEREAS the Canadian Association of Chiefs of Police (CACP) fully endorse the principles and values of integration and intelligence-led policing, and;

WHEREAS Canadians are concerned about the growing and pervasive threat of organized crime in their communities, and;

WHEREAS in response to their concerns, and in cooperation with the Law Enforcement Community, the CACP Organized Crime Committee is currently implementing a governance model for which the setting of enforcement priorities at the municipal, provincial, regional and national levels based on the intelligence contained in the National Threat Assessment will be a key component.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police supports the efforts in the development and implementation of the integrated intelligence-led Canadian Law Enforcement Strategy to Combat Organized Crime; whereby enforcement priorities are recognized, based on the Provincial and National Threat Assessments, and acted upon at the municipal, provincial and federal level.

Government of Canada / Gouvernement du Canada

× Symbol of the

Office of the Federal Ombudsman for Victims of Crime

Federal Ombudsman For Victims Of Crime Reacts To Proposed Changes To Internet Law

OTTAWA (Ontario), June 18, 2009 - Canada's Federal Ombudsman for Victims of Crime, Steve Sullivan, today joined Canada's Minister of Justice, Rob Nicholson and Canada's Minister of Public Safety, Peter Van Loan, to announce long-awaited changes to Canada's access laws. The new laws will make it mandatory for Internet Service Providers to give police basic customer information without a warrant when investigating online crimes, such as the creation or sharing of child sexual abuse material.

The Office of the Federal Ombudsman for Victims of Crime (FOVC) has pushed for change on this issue since it was created, and most recently made another formal recommendation to the government in its first special report *Every Image, Every Child* released earlier this month. The report, which addresses Internet-facilitated child sexual abuse, describes the issue in detail and presents arguments for why it is so important to grant police access to this information.

"We have heard from law enforcement across this country that not having access to this information is one of the biggest challenges they face in investigating cases and rescuing innocent children who are being violently sexually abused," explains Sullivan. "This change will help give authorities some of the tools they need to keep our children safe."

Currently in Canada, ISPs are allowed, but not obligated, to provide police who do not have a warrant with customer name and address information. While many ISPs do cooperate, 30 to 40 percent of requests are still being denied.

Previous public discussions on the issue have resulted in strong debate, as the issue is often misconstrued by critics as providing police with unwarranted and unlimited access to personal information and internet-surfing files.

"There has been a lot of dangerous misinformation and misunderstanding around this issue," says Sullivan. "The changes proposed will give police access to only the customer's basic information such as a name or an address, not to personal information like surfing history or banking records. It is in no way different than police looking up your name and address using your license plate number. This is not a privacy issue; it's a child safety issue."

To view FOVC's report *Every Image, Every Child*, or to learn more about the Office, visit the website at: www.victimsfirst.gc.ca

Created in 2007, the Office of the Federal Ombudsman for Victims of Crime helps victims to address their needs, promotes their interests and makes recommendations to the federal government on issues that negatively impact victims.

Media contact

For more information please contact:

Christina McDonald
Senior Communications Advisor
Telephone: 613-941-3428

SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report
2008–2009

Accountability in a new era of
security intelligence

Canada

Security Intelligence Review Committee
P.O. Box 2430, Station D
Ottawa, ON K1P 5W5
(613) 990-8441

Visit us online at www.sirc-csars.gc.ca

Collect calls are accepted between 8:00 AM and 5:00 PM, EST

Catalogue No. PS105-2009E-PDF

ISBN 978-1-100-13085-9

Security Intelligence Review Committee

Comité de surveillance des activités de renseignement de sécurité

September 30, 2009

The Honourable Peter Van Loan, P.C., M.P.
Minister of Public Safety
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Minister:

We are pleased to present you with the annual report of the Security Intelligence Review Committee for the fiscal year 2008–2009, as required by Section 53 of the *Canadian Security Intelligence Service Act*, for your submission to Parliament.

Sincerely,

Gary Filmon, P.C., O.M.

Chair

Raymond Speaker, P.C., O.C.

Denis Losier, P.C.

Frances Lankin, P.C.

Arthur T. Porter, P.C., M.D.

P.O. Box / C.P. 2430, Station / Succursale "D"
Ottawa, Canada K1P 5W5
Tel: *613* 990-8441 Fax: *613* 990-5230

[redacted]

WHAT IS SIRC?

The Security Intelligence Review Committee (SIRC, or the Committee) is an independent review body that reports to the Parliament of Canada on the operations of the Canadian Security Intelligence Service (CSIS, or the Service). By conducting reviews of CSIS activities and by investigating complaints, SIRC provides assurance to Parliament that the Service investigates and reports on threats to national security in a manner that respects the rule of law and the rights of Canadians.

WHAT IS CSIS?

CSIS is responsible for collecting and analyzing security intelligence and other related information within Canada and abroad. It advises the Government of Canada on issues and activities that are a threat to national security. CSIS also provides security assessments to all federal departments and agencies, with the exception of the Royal Canadian Mounted Police.

See Appendix B of this annual report for more information on some of CSIS's key activities.

[redacted]

CONTENTS

MESSAGE FROM THE COMMITTEE MEMBERS

Security intelligence operates in an ever-changing environment. The nature and pace of that change today is on a scale that has not been seen for several decades in Canada and elsewhere. Faced with a diverse threat environment of state and non-state actors, increased foreign investigations, growing demands from government stakeholders, as well as numerous public inquiries and court decisions pertaining to national security, the world of security intelligence has become increasingly complex.

It is against this backdrop that the Security Intelligence Review Committee (SIRC, or the Committee) continues to serve Canadians to ensure the democratic accountability of one of our country's most secretive institutions. Our mandate remains firmly rooted in assuring Parliament that the Canadian Security Intelligence Service (CSIS, or the Service) investigates and reports on threats to national security in a manner that respects the rule of law and the rights of Canadians. However, the range of security intelligence-related issues that we must understand and review continues to evolve in nature and scope.

At SIRC, we take great pride in being an organization that makes full use of the range of tools at our disposal to fulfill our mandate. Through the *Canadian Security Intelligence Service Act* (*CSIS Act*), Parliament gave this Committee a broad mandate to review the Service's performance in carrying out its duties and functions. Since it was first established in the 1980s, SIRC has endeavoured to fulfill this responsibility by responding to the changing priorities of CSIS and to the evolving expectations of Canadians for security intelligence in a democratic society. From the Committee's perspective, the *CSIS Act* has provided SIRC with a model framework to carry out its mandate.

Our annual report is a vital component of how we meet those expectations—maintaining a proud tradition of providing insight and analysis with probity and fairness. Given the nature and scope of the changes in the security intelligence environment, we feel this year is a fitting time to offer Canadians a new approach to the way we report our findings and recommendations.

This year's annual report includes an analysis section that identifies the main themes reviewed by SIRC in the past year and engages readers in a discussion about the importance of accountability in this new era of security intelligence. We are confident this undertaking will provide Parliament and all Canadians with a renewed understanding of SIRC's role in reviewing the operations of CSIS.

SIRC itself has also experienced important changes over the past year. We recently welcomed three new members to the Committee: the Honourable Frances Lankin, P.C., the Honourable Denis Losier, P.C., and the Honourable Dr. Arthur T. Porter, P.C., M.D. We all look forward to serving Canadians with the same level of commitment that has characterized SIRC's work since its inception. The Committee would also like to thank

[redacted]

Members of SIRC (from left to right), The Honourable Raymond Speaker, The Honourable Arthur T. Porter, The Honourable Gary Filmon (Chair), The Honourable Frances Lankin, The Honourable Denis Losier.
Photo: Couvrette/Ottawa

those members whose terms ended recently: the Honourable Roy Romanow, P.C., O.C., Q.C., the Honourable Baljit S. Chadha, P.C., and the Honourable Aldéa Landry, P.C., C.M., Q.C. We thank them for their dedication and wish all of them well in their future endeavours.

On a final note, the Committee would like to take this opportunity to send our best wishes to Jim Judd, who, after serving as the Director of CSIS, retired from the public service in June 2009. From our perspective, Mr. Judd conscientiously guided the Service through some of the most challenging issues that the organization has faced in recent years. All Members of SIRC extend their thanks to Mr. Judd for his professionalism in meeting with the Committee on a number of occasions to discuss CSIS's work and the state of security intelligence. We look forward to working with his successor, Mr. Richard B. Fadden, and wish him well in his new position.

We are proud to share with Parliament and all Canadians our summaries of reviews and complaints investigations undertaken during the 2008–2009 fiscal year. It is our hope that this annual report will help inform Canadians about SIRC's roles and responsibilities and the constructive role we play in ensuring that CSIS is effective in investigating and reporting on threats to national security, while respecting the rights and freedoms of citizens. This is an integral part of the scheme of accountability that was established in 1984 by Parliament—a framework that has stood the test of time, and a responsibility that we look forward to continuing to fulfill with great pride.

ABOUT THIS REPORT

SIRC provides assurances to Parliament—and through it, to Canadians—that CSIS investigates and reports on threats to national security in a manner that respects the rule of law and the rights of Canadians.

The *CSIS Act* gives SIRC full access to any information under the control of the Service. As a result, SIRC may examine all of CSIS's files and all of its activities—no matter how highly classified that information may be. The sole exception is Cabinet confidences (e.g., written and oral communications that contribute to the collective decision-making of Ministers).

This annual report summarizes SIRC's key analyses, findings and recommendations arising from its reviews and complaints investigations. It has three sections:

SECTION 1: THE YEAR IN REVIEW
An analysis of prominent developments within the security intelligence milieu, and of how these relate to select findings and recommendations by SIRC from the past year.

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS
A synopsis of reviews completed by SIRC as well as the complaint reports it has issued during the period covered by this report.

SECTION 3: SIRC AT A GLANCE
Details about the outreach, liaison and administrative activities of SIRC, including its annual budget and expenditures.

A NEW LOOK FOR SIRC'S ANNUAL REPORT

As part of SIRC's ongoing efforts to understand and report on new challenges and responsibilities in security intelligence in Canada, a revised layout has been developed for the organization's annual report. Key elements of these changes include:

MORE IN-DEPTH ANALYSIS FROM SIRC
The revised SIRC report explores the changing environment in which security intelligence operates. This includes observations about key trends and challenges that CSIS will need to address in the coming years.

EASY ACCESS TO FACTS AND RECOMMENDATIONS
This report features a revised layout to help you find the facts and information you're looking for, including: recommendations made during the review period and important information on the Committee.

BACKGROUND INFORMATION WHEN AND WHERE YOU WANT IT
Look for the caption boxes throughout this report. These contain valuable background information on various legal- and policy-related matters regarding SIRC's review and complaints functions.

SECTION 1: THE YEAR IN REVIEW

In less than two decades, the global environment in which Canada's security intelligence operates has undergone a fundamental transformation.

The end of the Cold War appeared to promise a more peaceful world with an expanding number of democracies and more widespread economic prosperity. It soon became clear, however, that the emerging global environment was both more complex and less secure than when there was a clear demarcation of interests between Western and Communist states.

The rise of global terrorism has played a significant role in shaping today's world, underscored most prominently by the rise of al Qaida as a globally capable terrorist platform. The 9/11 attacks on the United States, along with subsequent attacks in Europe and Asia, have changed how countries around the world perceive, and respond to, terrorism's destructive potential.

The contemporary threat environment is characterized by a constant danger of meticulously planned terror attacks designed to inflict mass casualties and destroy infrastructure. Canada has been openly threatened with attacks by al Qaida. It has also been subject to domestic and self-radicalizing terrorist cells. The arrest and trial of the Toronto 18 is reflective of this complex and evolving threat environment.

SIRC recognizes that CSIS must respond to these terrorist threats while still pursuing its traditional counter-intelligence priorities. For example, investigating the national security implications of the clandestine activities of foreign governments remains an important issue of concern. Likewise, counter-proliferation continues to be a top CSIS priority as the global community faces a number of unstable regimes with nuclear ambitions.

As the threat environment in which CSIS operates changes, so too does the corresponding legal environment. Recent court proceedings have lifted the veil of secrecy on the inner workings of the intelligence community. As part of this process, judicial rulings have required that the information CSIS brings to the courts meet the highest legal standards.

SIRC believes that the security intelligence environment will continue to be characterized by multiple threats and a high degree of unpredictability. Although global terrorism might shift its focus, it can be expected to continue to breed disorder and instability. Within this context, anticipating and defusing terrorist plans, while at the same time investigating other threats to national security, requires an effective security intelligence service.

When security agencies are faced with a multi-dimensional threat environment—and the need to protect society's fundamental values must be maintained—the role of a review body is equally complex. SIRC must comment on CSIS's capacity to carry out its mandate and on the tools that it has to undertake its work. Equally important, SIRC recommendations must be practical and reflect the values of Canadians.

SECTION 1: THE YEAR IN REVIEW

SIRC is the only independent review body with the mandate to comment on all aspects of the Service's operations. It can respond to complaints or, on its own initiative, review specific aspects of CSIS. It can also respond to requests from the Minister of Public Safety to review the Service's performance of its duties and functions.

Each year, SIRC reviews a selection of the Service's operational activities to determine if it acted appropriately, effectively and in accordance with the law. This year's annual report covers a range of CSIS's operational activities and deals with some of the complex issues that confront the Service. Section 2 of this report summarizes the Committee's reviews and complaint decisions.

In SIRC's view, CSIS has made important progress in developing policies to guide itself on human rights issues when investigating threats to national security. However, as SIRC's review of the Service's role in the matter of Omar Khadr reveals, there are additional issues to be addressed. Of particular note, CSIS must consider the principles of national and international law in regards to the treatment of minors when interviewing a Canadian detainee abroad.

Security agencies cannot investigate terrorist activities unless they exchange information efficiently across borders. Some of the countries that may possess vital intelligence on threats to Canada's security do not respect the human rights valued by Canadians. Canada does not use torture or approve of its use. Less straightforward, however, is whether CSIS should cooperate and interact with countries that may engage in human rights abuses to collect threat-related intelligence. As a result, it is increasingly important for SIRC to review the Service's interactions with foreign intelligence agencies.

A related issue arises if a CSIS representative interviews a Canadian detained abroad. The priority for CSIS is the collection of security intelligence. At the same time, it must consider suspicions of torture or other human rights abuses—whether a detainee is able to directly confirm them or not.

From SIRC's perspective, it is important for CSIS to address the many difficult issues that arise in conducting security intelligence work in a contemporary democracy. Most importantly, although intelligence collection is the Service's *raison d'être*, the Khadr review underscores how extra-intelligence matters must become an integral part of CSIS's decision-making processes. As part of this transition, CSIS must draw on the guidance of the Minister in addition to its own experience and resources.

In a separate review, the Committee examined CSIS's activities at Canadian airports. These locations can be targets for terrorist attacks because they concentrate large numbers of people and are a vital part of Canada's transportation infrastructure. CSIS activities at Canadian airports support the aviation security framework by providing national security advice and conducting interviews of persons suspected of posing a threat to national security. In reviewing the Service's activities at these airports, SIRC found that CSIS's presence enhances the security environment.

SIRC also examined the impact of legislation passed after 9/11 on CSIS's activities. For instance, one of the goals of the 2001 federal *Anti-Terrorism Act* (*ATA*, or the *Act*) was to address terrorism financing. However, the *Act* raised some difficult issues for CSIS in terms of managing its human source program. In particular, due to the *ATA's* provisions, activities related to CSIS's human source program that could benefit organizations listed as terrorist entities were, by definition, potentially criminal acts. Although CSIS has taken steps to address these issues, SIRC believes more accountability to the Minister of Public Safety is needed with respect to certain aspects of the Service's human source program.

SIRC's review of CSIS's investigation into domestic extremism found that key elements of the Service's strategy for dealing with the domestic threat environment needed to be reviewed and reformulated. The Committee believes this is necessary to ensure there is a clear and common understanding of both the threat environment and the terminology used to describe it. This task will become more pressing over the coming months in advance of the 2010 Olympic and Paralympic Winter Games in Vancouver—an event that will be a major test of Canada's security infrastructure.

SIRC has the power to comment on the manner in which CSIS has used its authorities, as well as whether those authorities are fair, reasonable and appropriate to the threat. The Committee's review of CSIS's Scientific and Technical Services commented on the continuing lack of lawful-access legislation and its impact on Service operations. This legislation is needed. It would require that Internet service providers include intercept capabilities in their networks. SIRC hopes that the government's latest legislative efforts on this matter are successful in achieving this goal.

The role of SIRC as a review agency would be straightforward if there were public successes and failures that could be analyzed for lessons learned. In the fortunate absence of an actual attack or a major security incident, SIRC examines aspects of CSIS operations, which can serve as valid indicators of the organization's capability, efficiency and effectiveness.

In the past, SIRC focused much of its review activity on CSIS operations within Canada. As CSIS moves to expand its capacity to operate outside of Canada, SIRC will accordingly allocate more of its resources to review these activities. As well, SIRC will continue to investigate complaints—not only to see if they are justified, but to determine whether they signal more systemic issues for review.

Because of its extensive powers to investigate CSIS, SIRC takes very seriously the duty to understand the complex challenges that CSIS confronts and to thoroughly review its activities.

SIRC's annual report is a vital component in meeting this expectation—one that has been entrusted to SIRC by Parliament, on behalf of Canadians.

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

A. REVIEWS

For more than 25 years, SIRC's reviews have provided Parliament and Canadians with a comprehensive picture of the Service's operational activities. It has also scrutinized CSIS's performance of its duties and functions to determine if the Service acted appropriately, effectively and in accordance with the law.

SIRC's reviews provide a retrospective examination and assessment of specific CSIS investigations and functions. The Committee's reviews include findings and—where appropriate—recommendations for the Service. Upon completion, all reviews are forwarded to both the Director of CSIS and the Inspector General of CSIS. SIRC is also authorized to provide special reports to the Minister of Public Safety on any matter that the Committee identifies as having special importance or that the Minister asks SIRC to undertake.

SIRC'S EARLIER REVIEWS

In past years, SIRC has reviewed a wide range of CSIS activities. For example, SIRC has examined how the Service carries out its mandate abroad by looking at activities undertaken at its various Stations around the world, the activities and investigations of CSIS regional offices, CSIS's cooperation and exchanges of information with domestic and foreign partners and specific operational activities such as CSIS's use of human sources. A complete listing of SIRC's past reviews can be found on the Committee's website (www.sirc-csars.gc.ca).

SIRC's research program is designed to address a broad range of subjects. In deciding which matters to review, SIRC considers:

- events with the potential to represent threats to the security of Canada;
- particular activities by CSIS that could have an impact on individual rights and freedoms;
- priorities and concerns identified by Parliament or in the media;
- issues identified in the course of SIRC's complaints functions;
- new directions or initiatives announced by, or affecting, CSIS;
- the CSIS Director's annual classified report submitted to the Minister of Public Safety; and
- the need to assess regularly each of the Service's branches and regional offices.

[redacted]

Each review results in a snapshot of the Service's actions in a particular context. This approach allows SIRC to manage the risk inherent in being able to review only a small number of CSIS activities in any given year.

SIRC's researchers consult multiple information sources to examine specific aspects of the Service's work. As part of this process, researchers may arrange briefings with CSIS employees, as well as examine individual and group targeting files, human source files, intelligence assessments and warrant documents, plus files relating to CSIS's cooperation and operational exchanges with foreign and domestic agencies and partners, among other sources that vary between reviews. The goal is to create a diverse pool of information so that SIRC can ensure it has thoroughly reviewed and completely understood the issues at hand.

ACCOUNTABILITY MATTERS

SIRC is one of several mechanisms designed to ensure CSIS's accountability. In addition to the reviews and complaints investigations conducted by the Committee, the Service also remains accountable for its operations through the Minister of Public Safety, the courts, the Inspector General of CSIS, central agencies of government (e.g., Privy Council Office, Treasury Board Secretariat), the Auditor General, the Information Commissioner and the Privacy Commissioner of Canada.

SIRC Review: CSIS's Role in the Matter of Omar Khadr

CONTEXT

Many Canadians are familiar with the story of Omar Ahmed Khadr—a Canadian citizen held at the United States detention facility at Guantanamo Bay, accused of killing a United States army medic during a firefight in Afghanistan in 2002. The American legal case against Khadr, his treatment while in US custody, his status as a child soldier, and the Canadian government's stance on his repatriation—all of these topics have garnered widespread media coverage and commentary. In July 2008, Khadr's story was thrust onto the international stage when his lawyers released a videotape showing CSIS officials interviewing their client at Guantanamo Bay in February 2003. The video prompted questions in the public domain about the nature and extent of CSIS's involvement in this matter, including the reasons for the Service's decision to interview Khadr.

SIRC'S LEGAL AUTHORITY IN THIS CASE

SIRC's review of CSIS's role in the matter of Omar Khadr was undertaken pursuant to Section 54 of the *CSIS Act*, which allows the Committee to forward to the Minister of Public Safety a special report on any matter that relates to CSIS's performance of its duties and functions. In most cases, these reports are reserved for matters that raise particularly difficult or high-profile issues that SIRC believes need to be brought to the Minister's direct attention. Examples of SIRC's previous Section 54 reviews include: the case of Mohammed Mansour Jabarah, the case of Maher Arar, the Heritage Front Affair, and CSIS activities in regard to the bombing of Air India Flight 182.

SIRC'S REVIEW

SIRC's objective was to conduct an in-depth review of CSIS's involvement in the case of Omar Khadr. The Committee looked back as far as mid-August 2002—when Canadian officials, including CSIS, were informed by American authorities that Khadr had been captured by US forces—to the federal court injunction in September 2005, prohibiting further interviews with Khadr by Canadian authorities.

In February and September 2003, CSIS officials travelled to Guantanamo Bay to meet with Khadr. SIRC noted that, from the Service's perspective, there were compelling operational reasons to interview him, given the threat posed by Sunni Islamic extremism in the months following 9/11. Khadr's father, Ahmed Khadr, was allegedly the highest-ranking Canadian al Qaida member. When the Americans granted Canadian intelligence and law enforcement officials access to Khadr, the Service seized the opportunity to gather intelligence that would advance their own investigation.

The driving force behind CSIS's interest in interviewing Khadr was to collect intelligence on a potentially serious terrorist threat and to provide advice to the Government of Canada accordingly. Although SIRC understands CSIS's position—that it had reasonable grounds to travel to Guantanamo Bay to gather threat-related information—the Committee found that the decision to interview Khadr was prompted primarily by intelligence considerations.

As a result, SIRC believes that CSIS failed to give proper attention to two important extra-intelligence matters: human rights issues and Khadr's age at the time that CSIS conducted its interview with him.

With respect to the first matter, SIRC examined the issues relating to the Service's handling of situations where it interacts and shares information with foreign partners when there are potential human rights considerations. CSIS's exchanges and cooperation with foreign

partners have come under closer scrutiny since 9/11, as it has become apparent that intelligence agencies need to work together to combat terrorist threats that transcend geo-political boundaries. Although information-sharing with foreign partners is crucial for CSIS to fulfill its mandate, it has created some new difficulties, specifically when working with countries that do not share Canada's respect for human rights.

The Canadian government fully supported CSIS's visit to, and interview of, Khadr at Guantanamo Bay in February 2003, as this initiative was part of a whole-of-government effort to gain access to him while in detention.

When CSIS interviewed Khadr in February 2003, there was widespread media reporting of alleged mistreatment and abuse of detainees in US custody in Afghanistan and at Guantanamo Bay. In mid-2002, allegations were made by several individuals relating to their treatment by American soldiers after being taken into custody in Afghanistan in late 2001 and 2002. Meanwhile, the US detention facility at Guantanamo Bay opened its door amid controversy as many countries denounced the American government's legal position, as well as its treatment of detainees.

SIRC did not find any evidence that CSIS took this into account in deciding to interview Khadr.

As a result of recommendations made by SIRC in 2004, and by Justice O'Connor in 2006 with respect to the case of Maher Arar, CSIS revised its policies governing the circumstances in which it shares information with foreign partners who are suspected of having questionable human rights records. CSIS and the Department of Foreign Affairs and International Trade (DFAIT) also signed a new protocol in 2007, to promote greater coordination and coherence across government in addressing issues that arise from consular cases involving Canadians detained abroad in cases related to suspected terrorism or national security. SIRC hopes that these developments will assist CSIS in the future in collecting intelligence while respecting human rights—particularly if confronted with situations similar to that of Khadr.

The second matter relates to Khadr's age. It is well recognized in Canadian and international law that youth are entitled to certain fundamental rights because of their status as a minor. In Canada, this is expressed in provisions of the federal *Youth Criminal Justice Act*. The rights of children are also reflected in international conventions to which Canada is party, such as the *UN Convention on the Rights of the Child*.

NO EASY SOLUTIONS

The issues raised in this case—such as information-sharing with foreign partners, human rights concerns when dealing with youth, and interacting with detainees in foreign jurisdictions—do not present simple remedies or easy answers. New mechanisms have been established to encourage CSIS to consider such issues as part of its decision-making process. However, in SIRC's view, it is becoming apparent that finding a solution to many of these complex post-9/11 issues will entail a thorough rethinking of intelligence work in light of recent social, policy and legal decisions.

SIRC found no evidence that CSIS, in deciding to meet Khadr at Guantanamo Bay, took into account the fact that their interview subject was still a youth at the time. In addition, youth radicalization is of growing concern to the Service. In light of these facts, SIRC recommended that the Service consider establishing a policy framework to guide its interactions with youth. As part of this, CSIS should ensure that such interactions are guided by the same principles that are entrenched in Canadian and international law.

Overall, SIRC believes that information-sharing with countries that have poor human rights records will continue to be a difficulty for CSIS until the Government of Canada resolves its seemingly contradictory position on information obtained from torture, versus the directions it provides to CSIS on carrying out its work.

This position places CSIS in an uncertain and vulnerable position when legal proceedings arise. Such was the case in the matter of Omar Khadr, in which Canadian courts found that DFAIT and CSIS had violated Khadr's *Charter* rights by interviewing him and submitting the resulting information to US investigators. Underpinning the courts' message is that CSIS can no longer view the activities it undertakes strictly through the lens of intelligence-gathering. It must also consider the wider environment and implications within which its work is carried out.

There is general agreement among intelligence experts and academics that the world of intelligence changed dramatically after 9/11. Although CSIS has taken important steps to tackle some of these resulting challenges, the matter of Omar Khadr suggests that changes in policies and procedures are but one component of a broader transition that needs to take place.

The time may have come for CSIS to undertake a fundamental reassessment of how it carries out its work, and shift its operational culture to keep pace with the political and legal developments of recent years. It is also important for the Service to demonstrate that it has the professionalism, experience and know-how required to make the difficult

decisions that arise when conducting operations abroad. Indeed, there is mounting pressure and expectation on CSIS to consider extra-intelligence matters in fulfilling its mandate and carrying out its activities.

RECOMMENDATIONS IN BRIEF

This review had two recommendations:

- The Service should consider establishing a policy framework to guide its interactions with youth. As part of this, CSIS should ensure that such interactions are guided by the same principles that are entrenched in Canadian and international law.
- CSIS should implement measures to embed the values stemming from recent political, judicial and legal developments in its day-to-day work to maintain its own credibility, and to meet growing and evolving expectations of how an intelligence agency should operate and perform in a contemporary democratic society. Guidance and advice from the Minister of Public Safety on how to accomplish this task would be helpful.

SIRC Review: CSIS's District Office Activities at Canadian International Airports

CONTEXT

A safe and secure civil aviation system is a vital component of Canada's economy. Its security is therefore of great importance. Following the 1985 bombing of Air India Flight 182 and the 9/11 terrorist attacks, a number of new measures were introduced across Canada to improve aviation security. These included new rules for aircraft and airport construction, enhanced screening of people and goods at airports, requirements for air carriers to provide basic information on specific passengers or flights, and assigning undercover police officers to provide security on Canadian aircraft. Although not an exhaustive list, these initiatives illustrate how civil aviation security has evolved into a broad network of players and responsibilities involving regional, provincial and federal agencies, as well as air carriers and private security firms.

SIRC'S REVIEW

CSIS plays an essential role within the complex web of airport security stakeholders by investigating threats to national security, as well as screening passengers travelling to Canada or airport employees requiring access to restricted areas. In addition, CSIS activities at Canadian airports support the aviation security framework in their respective regions.

For this review, SIRC examined CSIS's activities at a selection of Canadian airports. The objective was to better understand and assess the role of CSIS at these airports, including how they manage their airport-related responsibilities and work with their airport partners.

Through constant contact with airport stakeholders, service personnel are able to transfer information to regions and headquarters, and act as conduits for information collection and sharing among airport partners. The effectiveness of their communications depends on maintaining solid relationships. SIRC observed that both of CSIS's District Offices spent considerable time and effort developing and maintaining contact with both government and non-governmental airport stakeholders.

Further, SIRC observed that government and law enforcement partners in the airport environment frequently request the assistance of CSIS personnel to obtain national security advice related to airport operations. CSIS airport personnel are called on by airport stakeholders to provide briefings on threat-related issues, including information concerning CSIS's national security mandate. Service personnel also provide advice to law enforcement agencies in response to any security breach or criminal incident occurring at an airport where a risk to national security is suspected. Airport immigration officers, as part of CSIS's role in the Port of Entry Interdiction Program, also request the presence of CSIS personnel when conducting interviews of air travellers who are suspected of posing a potential threat to national security. During these interviews CSIS personnel conduct background checks to determine if the person has a history of threat-related activities. This expert advice is vital in securing airport entry points.

CSIS staff also spend considerable time and effort building and maintaining relationships within the airport environment. Through the development of these relationships, CSIS airport personnel are able to support regional and headquarters operational desks that require access to the airport infrastructure to carry out operations.

SIRC noted that CSIS staff who carry out activities at airports would benefit from greater exchanges with their counterparts who serve airports in other regions of Canada, and who carry out day-to-day functions similar to their own. SIRC believes that Service personnel whose main functions are to support airport security should be given the opportunity to collaborate and share best practices with their counterparts at other airports.

Overall, SIRC found that CSIS activities at airports reinforce the Service's national security mandate. Moreover, this provides airport stakeholders with readily available access to CSIS expertise.

RECOMMENDATIONS IN BRIEF

There were two recommendations arising from this review:

- CSIS should support efforts that encourage greater collaboration between Service personnel to enhance their operational activities at Canadian airports.
- The Service should ensure that their disaster management plans include activities at airports, so that procedures are in place to better ensure that the essential services that they provide are not interrupted in the event that their offices are rendered inoperable.

SIRC Review: A CSIS Human Source Operation

CONTEXT

CSIS's human source program is considered to be an effective and cost-efficient intelligence tool. Sources under this program are often able to provide insight about a target's intentions—something that cannot be gained through the Service's other methods of information gathering.

Legislative steps taken to date to fight terrorism have presented the Service with unique challenges in terms of the management of the human source program. One such challenge arose as a result of the *Anti-Terrorism Act* (2001). Due to its provisions, activities related to CSIS's human source program that could benefit organizations listed as terrorist entities were, by definition, potentially criminal acts.

ABOUT THE *ANTI-TERRORISM ACT*

The *Anti-Terrorism Act* gives the Government of Canada legal authority to create a list of entities believed to be involved in terrorist activities. The *Act* also makes it a criminal offence to, among other things, directly or indirectly collect or make available property or financial or other related services knowing they will be used by—or will benefit—a terrorist group.

Aware of the legal complexities of this situation, CSIS determined that its human source program was carried out within the confines of the law.

SIRC'S REVIEW

The Committee had briefly examined this issue in previous reviews. At that time, SIRC accepted the Service's position that CSIS operational policy was sufficient to cover all aspects of human source management. Nevertheless, SIRC maintained that it would continue to monitor the matter to identify challenging issues when required.

As part of this commitment, SIRC believed it was important to re-examine the matter at this time. For this review, SIRC placed special emphasis on the appropriateness and adequacy of the human source program's level of accountability within CSIS, and to the Minister of Public Safety.

In terms of accountability within CSIS, operational policy has not been updated to include any of the emerging factors that must be considered prior to determining whether actions carried out within the human source program are lawful. Nevertheless, SIRC found that a reporting structure was in place to ensure meaningful discussions take place within the Service about significant matters affecting management of the human source program.

In terms of accountability to the Minister of Public Safety, SIRC found that as a result of CSIS's interpretation—and by extension, its implementation—of operational policy, there was no venue by which it could inform the Minister of the implications of the *Anti-Terrorism Act* on human source operations. SIRC suggested a process of regularly updating the Minister on this matter.

Since the passage of the *Anti-Terrorism Act*, the Government of Canada has listed over 40 entities. As Canada's list of terrorist entities grows longer, commensurate growth is expected in the number of CSIS human source operations that could benefit listed organizations. It is important that CSIS be held to account for these activities.

RECOMMENDATIONS IN BRIEF

There was one recommendation arising from this review:

- CSIS should inform the Minister of Public Safety of the implications of the *Anti-Terrorism Act* as it relates to the Service's human source program and any future related developments.

SIRC Review: CSIS Activities at a Foreign Station

CONTEXT

In fulfilling its legal and operational responsibilities, CSIS maintains a presence outside of Canada. With the exception of three CSIS Stations—London, Paris and Washington—the locations are classified. Traditionally, the primary function of each Station was to liaise with CSIS's foreign partners and to conduct immigration screening. In addition, CSIS officials at headquarters used to manage operations abroad. Today, however, CSIS Stations take on larger roles in these operations. This expanded role coincides with an increase in the number of CSIS operations abroad, as underlined by former CSIS Director Jim Judd, who publicly acknowledged the Service's involvement in operations in Afghanistan, Iraq and Lebanon.

SIRC'S REVIEW

This year, the Committee examined the activities of a CSIS Station responsible for the Service's relationships with agencies in a number of countries. While not one of CSIS's busiest Stations, its work suggested that there was a high level of cooperation and information sharing. Although the Station under review was actively involved in operations, most continued to be managed by Canadian-based officials. Therefore, liaison work remained the Station's mainstay. Nevertheless, SIRC noted that the Station is well positioned to fulfill its mandate in liaison and operations.

To be effective in managing foreign relationships, all CSIS Stations need to have efficient methods of exchanging information—both with CSIS and its partner agencies. SIRC identified three communications-related challenges at the Station under review. In two instances, the challenges posed an inconvenience but did not prevent the Station from doing its work. SIRC also noted that CSIS had already indicated that it is exploring options to address these matters.

The third challenge related to the exchange of information directly from CSIS Headquarters to foreign agency representatives—as opposed to the accepted practice of sending the information through the respective CSIS Station. SIRC indicated that it would like to see a more consistent use of the accepted practice for exchanging information (i.e., all messages should go through the respective CSIS Station).

When the Service engages in operations abroad, senior-level approval is required from within CSIS. In recent years, this approval process was delegated downwards. The new process, however, was ambiguous and in some instances led to an inconsistent approach when seeking approval. New processes were recently instituted by CSIS, but these were outside of the scope of SIRC's work during the period under review. Nevertheless, it is worth noting that, in SIRC's estimation, the devolution of authority is a significant development that warrants ongoing examination.

As CSIS Stations become more active operationally, they are addressing some of the needs that a separate foreign intelligence service would otherwise address. SIRC will continue to monitor the activities of both the Service and the Stations as they take on greater operational roles.

RECOMMENDATIONS IN BRIEF

There was one recommendation arising from this review:

- CSIS should ensure there is a more consistent use of the accepted practice for exchanging information with foreign partners in which all messages go through the appropriate CSIS Foreign Station.

SIRC Review: CSIS's Scientific and Technical Services

CONTEXT

Of all the strategies used by CSIS to collect and access information, those that are technology-based are considered to be the most resource-intensive. Designing and deploying these technologies requires a wide range of specialties including forensics, mechanical engineering, programming and laboratory analysis. These are all within the responsibilities of CSIS's Scientific and Technical Services (STS) Branch.

Although previous SIRC studies have examined aspects of the Service's technical operations, the Committee believed it was appropriate to conduct a more thorough analysis of what goes on behind the scenes within CSIS before an operation takes place.

SIRC'S REVIEW

The goal of this review was to better understand the nature and scope of the STS Branch's work, including the challenges it faces in completing its work and how it cooperates with various partners. Intelligence technology is a complex business that requires continued access to new talent and innovative research and development, as well as the ability to develop products in a timely fashion—all while dealing with budgetary constraints. The STS Branch manages these challenges by working with Government of Canada partners and contracting-out to industry.

During the review, it became apparent to SIRC that not all of the challenges STS faces are within its control to address. Primary among these is the need to keep pace with rapidly

developing technologies in a variety of disciplines. Associated with this is the absence of lawful-access legislation—requiring telecommunication service providers to design their products with built-in intercept capabilities. This is in sharp contrast to the experience of CSIS's counterparts in the United States and Europe, where governments have legislated cooperation between the service providers and security intelligence agencies.

In Canada, opponents to lawful-access legislation cite a number of concerns, including:

- the appropriateness of compelling service providers to create intercept solutions;
- the scope of information that would be obtained and how it would be used; and
- whether restrictions or oversight would exist to prevent abuse.

Canada's Privacy Commissioner has argued against various iterations of the proposed legislation, most recently stating that "lawful access raises fundamental issues for rights such as privacy and the ability to communicate freely." The Committee recognizes it is important that Canadians engage in a healthy debate on this issue. However, SIRC is concerned that STS's ability to perform certain investigative procedures will be constrained until the government is successful in enacting appropriate legislation.

On June 18, 2009, during preparation of SIRC's 2008–2009 Annual Report, the federal government tabled the *Technical Assistance for Law Enforcement in the 21st Century Act*. If enacted, this legislation would require that internet service providers include intercept capabilities in their networks. SIRC will follow the development of this legislation to determine its potential impact on the Service's intelligence-gathering mandate and priorities.

There were no recommendations arising from this review.

SIRC Review: CSIS's Investigation into Domestic Extremism

CONTEXT

The Government of Canada considers domestic extremism a national intelligence priority. For this reason, CSIS identifies domestic, politically motivated violence as one of its highest priorities. The investigation of domestic extremism, however, presents a unique challenge to the Service. While it must gather information required to fulfil its mandate, CSIS must also refrain from infringing on Canadians' protected rights to lawful advocacy, protest and dissent. Successfully negotiating the line between legal

protest and activist extremism requires a specialized and in-depth understanding of advocacy movements, protest tactics and the ways in which otherwise well-intentioned protesters can become radicalized.

SIRC'S REVIEW

This study had two objectives. First, SIRC examined CSIS activities in relation to domestic extremism, taking into account the overlap with criminal investigations and lawful advocacy, protest and dissent. SIRC found that CSIS had allocated appropriate resources to deal with the potential threat from domestic extremism. Moreover, CSIS had developed significant expertise regarding potential threats from domestic extremism, as well as a series of balanced measures to ensure Canadians' right to legal dissent.

However, SIRC found that some of the strategies employed by the Service to analyze the threat environment could benefit from reformulation. Several key concepts to evaluate the potential threat are not universally understood, commonly defined or used consistently. SIRC recommended that the Service establish an accepted terminology and gain a deeper understanding of the parameters of the threat environment to isolate and identify indicators of radicalization.

The second objective was to examine CSIS investigations of special events (i.e., an event that provides a heightened opportunity for carrying out threat-related activities). In that regard, the Committee examined the plans and priorities put in place by the Service for the 2010 Olympic and Paralympic Winter Games in Vancouver, and found them to be on-schedule and well-conceived. However, several of the concerns raised in the context of domestic extremism investigations—key concepts not being commonly defined or used consistently—applied equally to the Service's assessment of the threat environment surrounding the Olympic and Paralympic Games.

It is important to note that CSIS's understanding of the Olympics threat environment continues to evolve and its efficiency during the 2010 Games will depend on its ability to assess accurately the movements associated with domestic extremism. SIRC believes that the strategies recommended to address the concerns highlighted in the domestic extremism investigation will also inform CSIS's preparations for the Olympics.

RECOMMENDATIONS IN BRIEF

There was one recommendation arising from this review:

- CSIS should take steps to develop stronger definitions and a better understanding of the multi-issue extremism environment. The objective should be to build a more effective model to isolate and identify indicators of activist extremism and their potential for violence.

SIRC Review: The Case of Paul William Hampel

CONTEXT

Former CSIS Director Jim Judd has publicly acknowledged that foreign powers are becoming more sophisticated in conducting espionage within Canada's borders. A recent case of Russian espionage in Canada underlines this concern. In November 2006, a Russian spy, who had been using the name Paul William Hampel, was detained by Canadian officials in Montreal as he was about to board an international flight. The circumstances surrounding Hampel's detention received significant media attention, which reported that he was a Russian intelligence officer who had been residing in Canada under a false identity since 1995. However, there was no reporting of the nature and scope of CSIS's involvement in this high-profile and sensitive matter.

SIRC'S REVIEW

The objective of SIRC's review was to understand CSIS's involvement in the Hampel case. The Committee found that after becoming aware of Hampel's existence, CSIS conducted an investigation to determine the nature and scope of his espionage activities.

During the course of the investigation, the Service gathered important information to advise the Ministers of Public Safety and Citizenship and Immigration that Hampel was a known member of Russia's Foreign Intelligence Service and had used a fraudulent Canadian identity to further Russian espionage activities. In accordance with the *Immigration and Refugee Protection Act*, the Ministers signed a security certificate, thereby initiating the process by which Hampel was eventually deported to Russia.

As a result of the Hampel investigation, CSIS gained additional insights into the espionage threat posed to Canada by the activities of the Russian Intelligence Services. This will assist CSIS in investigating similar threats should they arise in the future.

There were no recommendations arising from this review.

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

B. COMPLAINTS

In addition to its review function, SIRC is responsible for investigating complaints about CSIS. Almost all complaint cases begin as inquiries to SIRC—either in writing, in person or by phone. In turn, SIRC staff respond promptly, usually instructing the prospective complainant about what the *CSIS Act* requires for a concern to become a formal complaint.

WHAT IS THE DIFFERENCE BETWEEN A REVIEW AND A COMPLAINT INVESTIGATION?

A **review** is initiated by SIRC and entails in-depth research of CSIS's performance in carrying out its duties as described in the *CSIS Act*. A **complaint** investigation is initiated by an individual or group who may make a complaint to SIRC with respect to: "any act or thing done by the Service" (Section 41); denials or revocation of security clearances to government employees or contractors (Section 42); referrals from the Canadian Human Rights Commission; and Minister's reports in regards to the *Citizenship Act*. While reviews constitute SIRC's research function, complaint investigations are conducted as part of a quasi-judicial process.

Once a written complaint is received, SIRC conducts a preliminary review. Where a complaint does not meet certain statutory requirements, SIRC declines jurisdiction and the complaint is not investigated. If jurisdiction is established, complaints are investigated through a quasi-judicial hearing presided over by one or more Committee Members, assisted by staff. A complainant has the right to be represented by counsel and to make representations at the hearing. Pre-hearings may be conducted to establish and agree on procedures with the complainant and/or the complainant's counsel.

SIRC's legal team provides advice on procedural and substantive matters, and will also cross-examine Service witnesses when, for national security reasons, evidence must be heard without the complainant being present.

TYPES OF COMPLAINTS

The types of complaints that SIRC investigates are described in the *CSIS Act* and take several forms. Under Section 41 of the *CSIS Act*, SIRC can investigate "any act or thing done by the Service." Under Section 42, it can hear complaints about denials of security clearances to federal government employees and contractors. Section 42 does not permit SIRC to accept jurisdiction to hear complaints concerning less intrusive background screening or reliability checks, which are conducted simply to determine the trustworthiness or suitability of a potential federal employee. These complaints are addressed through an organization's designated grievance procedure or potentially under Section 41 of the *CSIS Act*.

[redacted]

When SIRC's investigation of a complaint made under Section 41 is concluded, it provides a report to the Director of CSIS, the Minister of Public Safety and the complainant.[1] Summaries of these reports, edited to protect national security and the privacy of complainants, are also included in SIRC's annual report to Parliament.

Pursuant to Section 42 of the *CSIS Act*, individuals who have been denied a security clearance must be informed of this action by the Deputy Head of the organization. These individuals have the right to make a complaint to SIRC and, where appropriate, SIRC will investigate and report its findings and any recommendations to the Minister, the Director of CSIS, the Deputy Head concerned and the complainant.

Should the Canadian Human Rights Commission receive a written notice from a Minister of the Crown about a complaint that relates to the security of Canada, the Commission may refer the matter to SIRC. Upon receipt of such a referral, SIRC carries out an investigation and reports its findings to the Commission, the Director of CSIS, the Minister of Public Safety, the Minister of the department concerned and the complainant. SIRC also has the authority to conduct investigations into matters referred to SIRC pursuant to the *Citizenship Act*.

Table 1 provides the status of all complaints directed to SIRC over the past three fiscal years, including complaints that were misdirected to SIRC, deemed to be outside SIRC's jurisdiction, or investigated and resolved without a hearing (i.e., via an administrative review).

TABLE 1
RESOLUTION OF COMPLAINTS

	2006–07	2007–08	2008–09
Carried over	24	20	15
New	37	32	30
Total	**61**	**52**	**45**
Closed[†]	41	37	23
Carried forward to subsequent year	20	15	22
Reports issued	5	6	1

[†] Closed files include those where reports were issued, the Committee did not have jurisdiction, the preliminary conditions of the complaint were not met, or the complaints were withdrawn. In the past year, the Committee dealt with an increased number of files raising complex jurisdictional issues.

[1] The complainant receives a declassified version of the report.

HOW SIRC DETERMINES JURISDICTION OF A COMPLAINT...

...UNDER SECTION 41

Under Section 41 of the *CSIS Act*, SIRC shall investigate complaints made by "any person" with respect to "any act or thing done by the Service." Before SIRC investigates, two conditions must be met:

1. The complainant must first have complained in writing to the Director of CSIS and not have received a response within a reasonable period of time (approximately 30 days), or the complainant must be dissatisfied with the response; and
2. SIRC must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

SIRC cannot investigate a complaint that can otherwise be addressed under existing grievance procedures of the *CSIS Act* or the *Public Service Labour Relations Act.*

...UNDER SECTION 42

With respect to security clearances, Section 42 of the *CSIS Act* says SIRC shall investigate complaints from:

1. Any person refused federal employment because of the denial of a security clearance;
2. Any federal employee who is dismissed, demoted, transferred or denied a transfer or promotion for the same reason; and
3. Anyone refused a contract to supply goods or services to the government for the same reason.

These types of complaints must be filed within 30 days of the denial of the security clearance. SIRC may extend this period if valid reasons are presented.

SIRC Complaint: Investigation of Alleged Profiling

SIRC investigated a complaint in which the complainant was required to obtain an airport restricted-access security clearance for the purposes of employment. In this case, Transport Canada requested that CSIS undertake a security assessment to appraise this individual's loyalty to Canada and reliability as it relates to such loyalty. The complainant was subsequently contacted by CSIS and a security-screening interview was conducted.

In the complaint to SIRC, filed pursuant to Section 41 of the *CSIS Act*, the complainant alleged profiling by CSIS. In addition, the complainant objected to the use of questions during the interview, which the complainant alleged solicited political opinions and were believed prohibited under the *Charter of Rights and Freedoms*. The complainant sought an apology and written assurances that CSIS would stop asking these questions at future security-screening interviews.

For its part, CSIS argued that it is not unusual to conduct interviews as part of the security screening process. Interviews may be conducted for cause when it is determined that there is insufficient information regarding an individual to complete a security assessment. In conducting its security assessment, CSIS is required, as per the *CSIS Act*, to appraise a person's "loyalty to Canada and reliability as it relates to such loyalty." In doing so, it will consider a range of factors when completing these assessments, including personal beliefs and associations—matters the Service considers to be consistent with the Treasury Board Secretariat's Government Security Policy.

SIRC's investigation included a detailed review of CSIS's documentation, as well as testimony from the complainant and representatives from CSIS plus a Treasury Board Secretariat representative who spoke about the purpose of the Government Security Policy. As a result of this information, SIRC was satisfied that CSIS acted in accordance with the Government Security Policy, the Government Security Policy Standard, as well as CSIS's applicable operational policies in requesting that the complainant attend a security-screening assessment interview. In addition, SIRC found that the complainant was not profiled on grounds prohibited by the *Charter of Rights and Freedoms*, and found that questions in the security-screening interview relating to the complainant's opinions and beliefs did not infringe on the complainant's rights under the *Charter*.

SIRC'S LEGAL AUTHORITY TO INVESTIGATE COMPLAINTS

Under Section 41 of the *CSIS Act*, SIRC has the authority to investigate complaints made by "any person" with respect to "any act or thing done by the Service." The Committee must also be satisfied that the complaint is not trivial, vexatious or made in bad faith.

ABOUT THE GOVERNMENT SECURITY POLICY

The Government of Canada must ensure that individuals who have access to government information and assets are reliable and trustworthy. Ensuring loyalty to Canada is essential for protecting Canadians and Canadian assets from threats posed by terrorism and espionage, or from malicious or improper activities, such as the unauthorized disclosure of classified and protected information that can have a serious impact on the safety of Canadians and on the effective functioning of society. Federal departments must therefore ensure that individuals are appropriately screened before commencing their duties. CSIS plays a vital role in this process, providing security assessments for government departments and institutions (see Appendix B of this report for further information on CSIS's security screening activities.) For more details on the Government Security Policy, visit the Treasury Board of Canada Secretariat's website (www.tbs-sct.gc.ca).

SECTION 3: SIRC AT A GLANCE

COMMITTEE MEMBERSHIP

SIRC is chaired by the Honourable Gary Filmon, P.C., O.M., who was appointed as Chair on June 24, 2005. The other Committee Members are the Honourable Frances Lankin, P.C., the Honourable Denis Losier, P.C., the Honourable Dr. Arthur T. Porter, P.C., M.D., and the Honourable Raymond Speaker, P.C., O.C.

All Members of SIRC are Privy Councillors. Each is appointed by the Governor-in-Council after consultation by the Prime Minister with the leaders of the Opposition parties.

In addition to attending monthly committee meetings, members preside over complaints hearings, prepare reviews and complaint reports in consultation with SIRC staff, visit CSIS regional offices, address Parliamentary committees and exercise other duties associated with their responsibilities.

COMMITTEE ACTIVITIES

October 5–8, 2008: The Chair, the Executive Director, and a Member of SIRC attended the International Review Agencies Symposium, hosted in Auckland, New Zealand, by the Inspector-General Intelligence and Security.

October 30–November 1, 2008: The Executive Director and several staff attended a conference of the Canadian Association of Security and Intelligence Studies, held in Ottawa.

November 4, 2008: At Carleton University, the Executive Director gave a lecture to students of a course on national security, providing an overview of SIRC's role and mandate.

March 5, 2009: The Executive Director appeared before the House of Commons Standing Committee on Public Safety and National Security.

March 24, 2009: The Acting Senior Counsel and the Senior Advisor met with officials from the New Zealand Security Intelligence Service.

March 26, 2009: The Acting Senior Counsel and the Senior Advisor met with officials from the Intelligence Security Committee (United Kingdom).

[redacted]

STAFFING AND ORGANIZATION

SIRC is supported by an Executive Director, Susan Pollak, and an authorized staff complement of 20, located in Ottawa. The staff comprises a Senior Advisor, a Senior Counsel, a Corporate Services Manager, Counsel, a Senior Paralegal, plus researchers and administrative staff.

Committee Members provide staff with direction on research and other activities that are identified as a priority for the year. Management of day-to-day operations is delegated to the Executive Director with direction, when necessary, from the Chair as Chief Executive Officer.

As part of their ongoing work, the Chair of SIRC, Committee Members and senior staff participate in regular discussions with CSIS executive and staff, and other senior members of the security intelligence community.

These exchanges are supplemented by discussions with academics, security and intelligence experts and other relevant organizations. These activities enrich SIRC's knowledge about issues and opinions affecting national security intelligence.

SIRC also visits CSIS regional offices on a rotating basis to better understand and examine the day-to-day work of investigators in the field. These visits give Committee Members an opportunity to be briefed by regional CSIS staff on local issues, challenges and priorities. It is also an opportunity to communicate SIRC's focus and concerns.

During the 2008–09 fiscal year, SIRC visited three regional offices.

BUDGET AND EXPENDITURES

SIRC continues to manage its activities within allocated resource levels. Staff salaries and travel within Canada for Committee hearings, briefings and review activities represent its chief expenditures. Table 2 below presents a breakdown of actual and estimated expenditures.

TABLE 2
SIRC EXPENDITURES 2008–09

	2008–09 (Estimates)	2008–09 (Actual)
Personnel	$1,900,000	$1,700,000
Goods and Services	$1,000,000	$700,000
Total	$2,900,000	$2,400,000

APPENDIX A: LIST OF RECOMMENDATIONS

During the 2008–2009 review period, SIRC made the following recommendations stemming from the range of reviews it conducted, as well as from the complaint it investigated.

CASE[1]	SIRC RECOMMENDED THAT...
CSIS'S ROLE IN THE MATTER OF OMAR KHADR	The Service should consider establishing a policy framework to guide its interactions with youth. As part of this, CSIS should ensure that such interactions are guided by the same principles that are entrenched in Canadian and international law. CSIS should implement measures to embed the values stemming from recent political, judicial and legal developments in its day-to-day work to maintain its own credibility, and to meet growing and evolving expectations of how an intelligence agency should operate and perform in a contemporary democratic society. Guidance and advice from the Minister of Public Safety on how to accomplish this task would be helpful.
CSIS ACTIVITIES AT CANADIAN INTERNATIONAL AIRPORTS	CSIS should support efforts that encourage greater collaboration between Service personnel to enhance their operational activities at Canadian airports. The Service should ensure that their disaster management plans include activities at airports, so that procedures are in place to better ensure that the essential services that they provide are not interrupted in the event that their offices are rendered inoperable.
A CSIS HUMAN SOURCE OPERATION	CSIS should inform the Minister of Public Safety of the implications of the *Anti-Terrorism Act* as it relates to the Service's human source program and any future related developments.
CSIS ACTIVITIES AT A FOREIGN STATION	CSIS should ensure there is a more consistent use of the accepted practice for exchanging information with foreign partners in which all messages go through the appropriate CSIS Foreign Station.
CSIS'S INVESTIGATION INTO DOMESTIC EXTREMISM	CSIS should take steps to develop stronger definitions and a better understanding of the multi-issue extremism environment. The objective should be to build a more effective model to isolate and identify indicators of activist extremism and their potential for violence.

[1] Consult the SIRC website at www.sirc-csars.gc.ca for a list of all SIRC reviews conducted since 1984.

APPENDIX B: CSIS AT A GLANCE

Each year, as part of SIRC's annual report, the Committee presents important information and statistics related to CSIS operations. This data, provided by the Service, provides readers with insight into some of the Service's key duties and functions, as well as highlights any major changes or developments within CSIS.

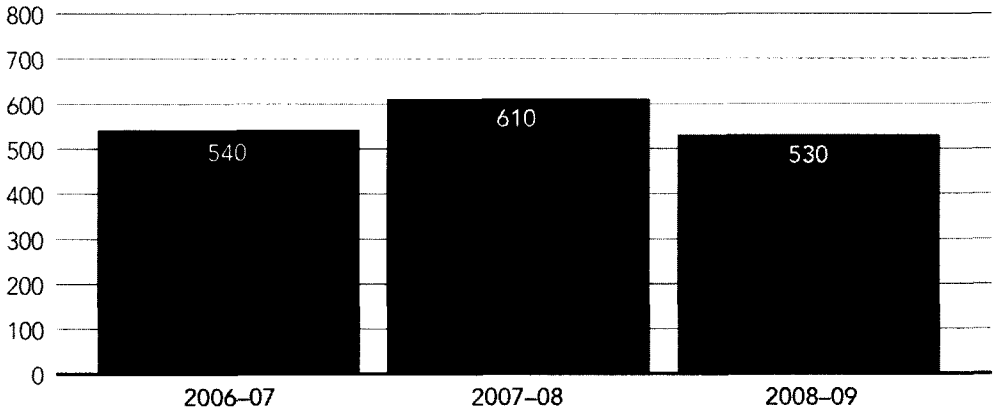
For SIRC's 2008–2009 Annual Report, this information is grouped in two categories: security intelligence activities and security screening activities.

A. SECURITY INTELLIGENCE ACTIVITIES

Targeting

When the Service has reasonable grounds to suspect that an individual or an organization could pose a threat to Canada, it must first establish an investigation in which it exercises its powers proportionate to the threat that is posed. Figure 1 indicates the number of targets investigated by CSIS during the period under review, relative to previous fiscal years.

FIGURE 1
TARGETING STATISTICS*



Note: * Figures have been rounded to the nearest 10.

Warrants

The power to authorize intrusive investigative techniques rests strictly with the Federal Court of Canada. If the Court grants a warrant, it provides CSIS with authorization to use investigative techniques that would otherwise be illegal, such as the monitoring of telecommunications activities. Table 3 shows the number of federal court-approved warrants that CSIS had during the period under review, relative to previous years.

TABLE 3
WARRANT STATISTICS

	2006–07	2007–08	2008–09
New warrants	42	71	26
Replaced or renewed	134	182	183
Total	176†	253††	209†††

† Included in this number were 25 urgent warrants.

†† Included in this number were 19 urgent warrants.

††† Included in this number were 2 urgent warrants.

B. SECURITY SCREENING ACTIVITIES

Security screening is one of the most publicly visible functions provided by CSIS. This activity consists of government screening (which includes site-access screening) and immigration screening.

Government screening

This type of screening provides security assessments—an appraisal of the loyalty to Canada and (so far as it relates thereto) the reliability of an individual—for all government departments and institutions, except the Royal Canadian Mounted Police (RCMP).

CSIS does not decide who receives a security clearance. Rather, it advises the requesting department or agency of information that could have an impact on their decision to grant a clearance. On rare occasions, CSIS will recommend to a requesting agency that the threshold in the Government Security Policy has been met to deny a clearance. However, it is the responsibility of the requesting agency to grant, revoke or deny a clearance.

Table 4 reports the number of requests for government screening that CSIS received over a three-year period. Table 5 reports the median turnaround time for CSIS to complete these assessments.

TABLE 4
REQUESTS FOR CSIS GOVERNMENT SECURITY SCREENING*

	2006–07	2007–08	2008–09
Requests from Department of National Defence (DND)	13,100	8,800	15,300
Requests from other clients	38,100	41,500	46,400
Total	51,200	50,300	61,700
Assessments issued to DND	13,100	8,300	14,400
Assessments issued to other clients†	41,800	40,500	46,300
Total	54,900	48,800	60,700

* Figures have been rounded to the nearest 100.

† This number includes assessments performed for provincial governments and for access to nuclear facilities.

TABLE 5
MEDIAN TURNAROUND TIME (IN CALENDAR DAYS) FOR CSIS TO COMPLETE SECURITY ASSESSMENTS

		2006–07†	2007–08		2008–09	
			New	Updates	New	Updates
DND	Level I (Confidential)	40	23	9	74	57
	Level II (Secret)	40	28	23	61	62
	Level III (Top Secret)	82	164	29	126	57
Non-DND	Level I (Confidential)	32	18	13	18	6
	Level II (Secret)	21	13	12	15	16
	Level III (Top Secret)	47	186	4	145	8

† For 2006–07, median turnaround times for new and update security assessments were not available. The time reported in this column therefore is for both types of assessments.

Site-access screening

This type of screening allows an individual access to certain secure areas—such as airports, port and marine facilities, the Parliamentary Precinct and nuclear power facilities—and provides accreditation for special events and assessments to provincial departments. These programs are meant to enhance security and reduce the potential threat from terrorist groups and foreign governments, which may seek to gain unauthorized access to classified information or other assets, materials and sensitive sites. Table 6 reports the number of requests that CSIS received for site-access screening over the past year, relative to the previous two years.

TABLE 6
REQUESTS TO CSIS FOR SITE-ACCESS SCREENING*

	2006–07	2007–08	2008–09
Parliamentary Precinct	1,100	1,100	1,000
Airport restricted-access area (Transport Canada)	39,300	36,800	31,400
Nuclear facilities	17,900	9,200	11,100
Free and Secure Trade (FAST)	23,100	10,700	6,400
Special events accreditation	0	1,300	16,300
Marine Transportation Security Clearance Program†	N/A	6,300	5,200
Other government departments	2,500	2,100	2,600
Total	83,900	67,500	74,000

* Figures have been rounded to the nearest 100.

† The Marine Transportation Security Clearance Program became operational in December 2007 to provide security assessments in relation to the security of Canada's ports.

Immigration screening

This type of screening helps to ensure that individuals who pose a threat to security and/or are inadmissible under the *Immigration and Refugee Protection Act* do not gain entry or obtain status in Canada. If an individual meets one or more of these criteria, CSIS will issue a brief. Table 7 reports the number of citizenship and immigration screening requests received by CSIS, as well as the number of briefs issues in relation to these requests.

TABLE 7
REQUESTS TO CSIS FOR CITIZEN AND IMMIGRATION SCREENING AND BRIEFS ISSUED

	Requests*			Briefs		
	2006–07	**2007–08**	**2008–09**	**2006–07**	**2007–08**	**2008–09**
Permanent resident†	62,800	66,000	67,300	201	195	213
Front-end screening††	17,900	21,800	26,800	143	117	108
Refugee determination†††	11,600	6,600	6,600	153	142	102
Subtotal	**92,300**	**94,400**	**100,700**	**497**	**454**	**423**
Citizenship applications	227,300	190,000	169,500	155	109	169
Total	319,600	284,400	270,200	652	563	592

* Figures have been rounded to the nearest 100.

† This includes permanent residents inside and outside Canada (excluding the Refugee Determination Program), permanent residents from within the United States and applicants from overseas.

†† Individuals claiming refugee status at inland offices or at ports of entry.

††† Refugees, as defined by the *IRPA*, who apply from within Canada for permanent resident status.

APPENDIX B: CSIS AT A GLANCE

Table 8 reports the time it took for CSIS to complete notices of assessment, which are issued in those government and immigration screening cases when CSIS finds no adverse information on an applicant.

TABLE 8
TURNAROUND TIME (IN DAYS) FOR CSIS TO COMPLETE NOTICES OF ASSESSMENT

	2006–07	2007–08	2008–09
Citizenship	1	1	1
Immigration (Canada)†	78	59	95
Immigration (USA)††	29	45	65
Overseas immigration	14	20	26
Refugee determination	98	64	89
Front-end screening	19	28	29

† This includes certain classes of individuals who apply for permanent resident status from within Canada.

†† This includes persons who have been lawfully admitted to Canada for at least one year and who may submit their application to Citizenship and Immigration offices in the United States.

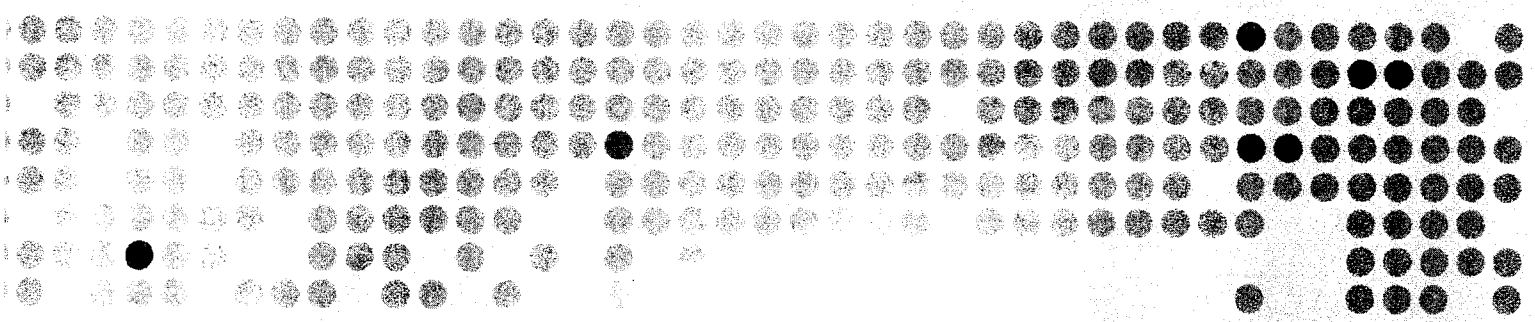
Office of the Federal Ombudsman
Government of Canada
Bureau de l'ombudsman fédéral
Gouvernement du Canada

Heard. Respected. Victims First.
Écoutées. Respectées. Les victimes d'abord.

Every Image, Every Child

INTERNET FACILITATED CHILD SEXUAL ABUSE IN CANADA

Canada



OFFICE OF THE FEDERAL OMBUDSMAN FOR VICTIMS OF CRIME

In March 2007, the Ministers of Justice and Public Safety announced the creation of the Office of the Federal Ombudsman for Victims of Crime to ensure the federal government meets its responsibilities to victims of crime.

As part of its mandate, the Office identifies emerging issues that impact negatively on victims of crime and makes recommendations to Parliament based on those issues and the principles set out in the *Canadian Statement of Basic Principles of Justice for Victims of Crime.*

This report is part of that important work.

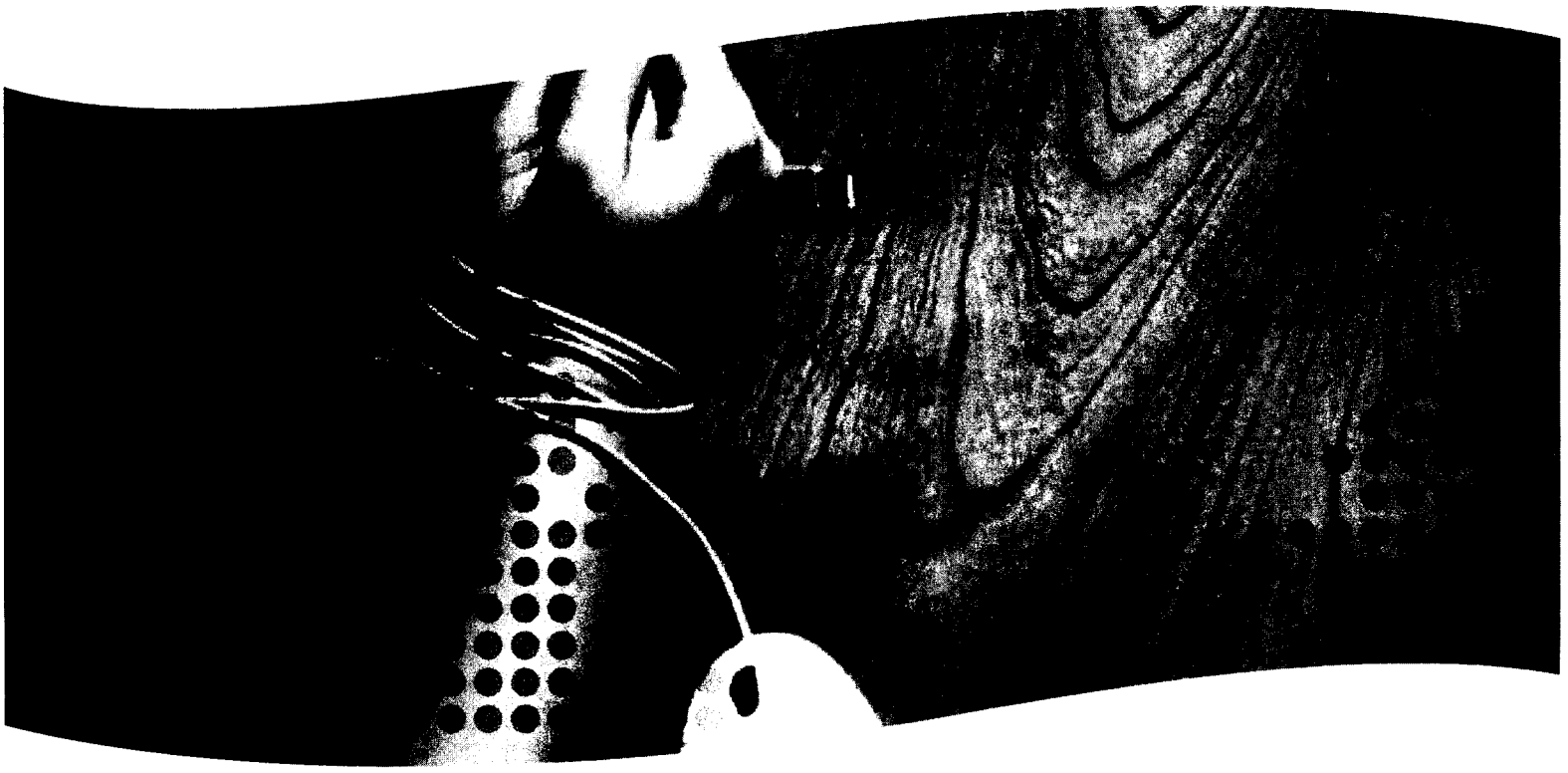
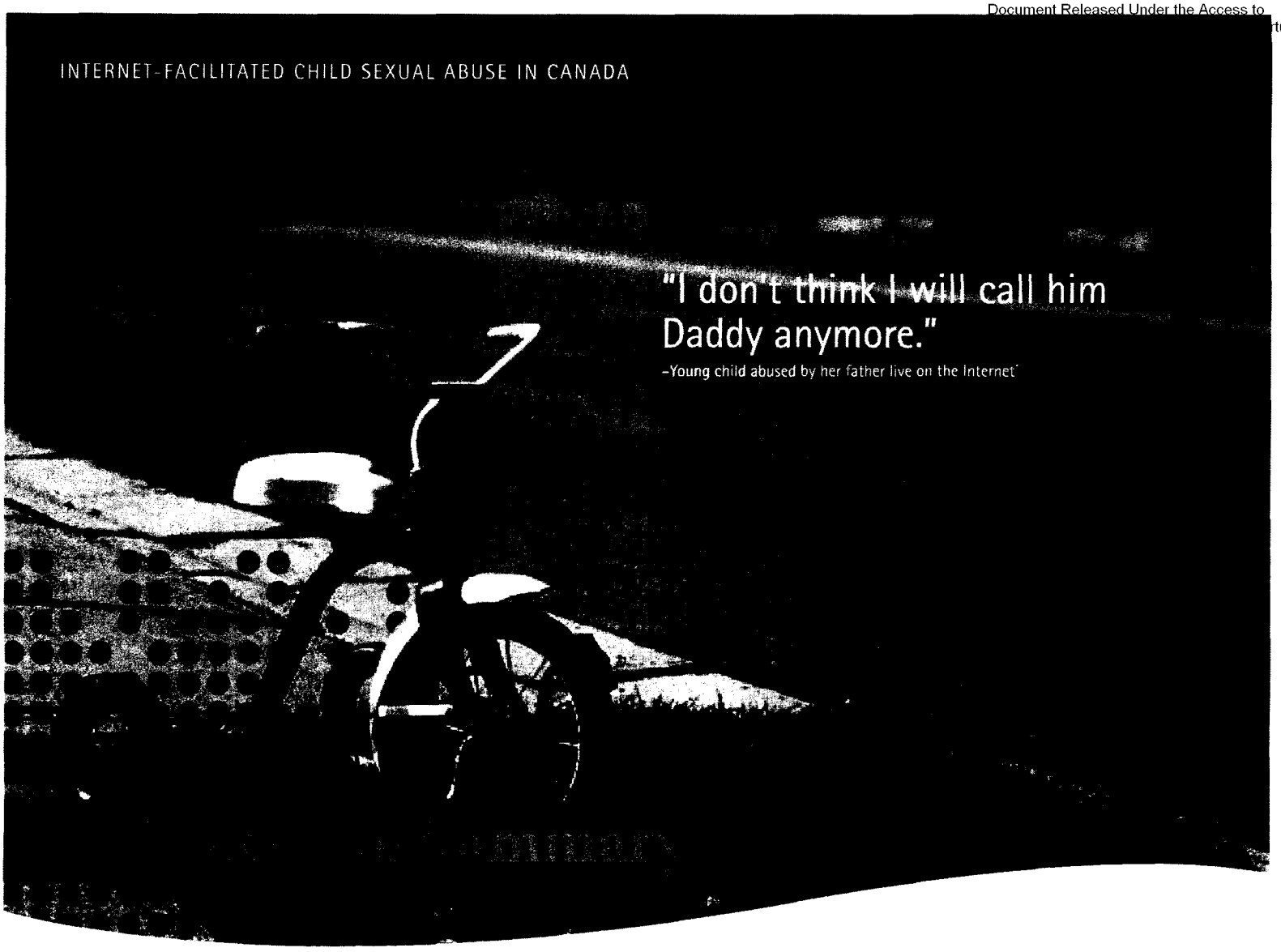


Table of Contents



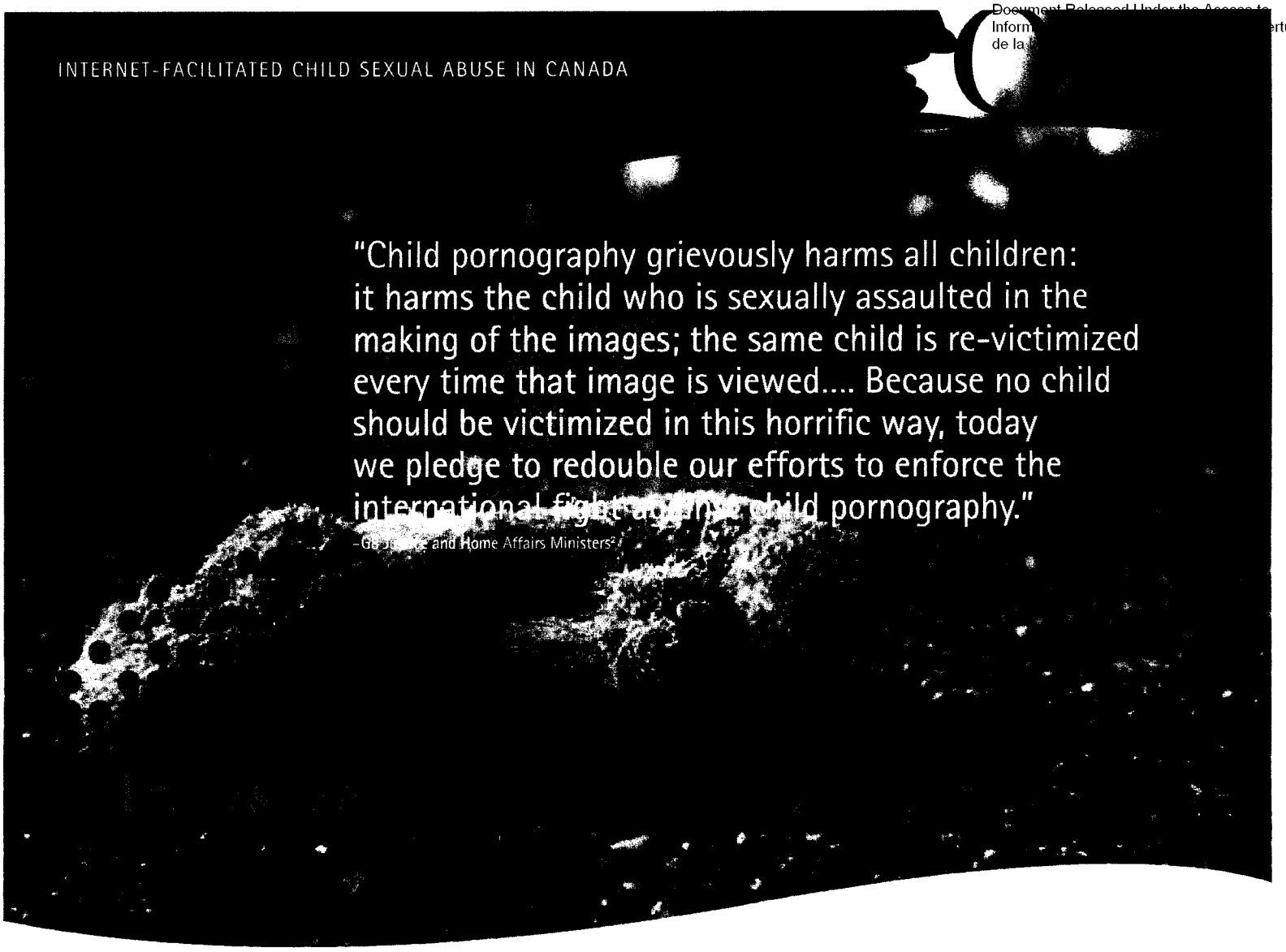
EVERY IMAGE, EVERY CHILD gives an overview of the problem of Internet-facilitated child sexual abuse, provides limited historical information about what has been done by the federal government on the issue to date, identifies issues that negatively impact child victims and makes nine recommendations for positive change.

The nine recommendations touch on:

- the term "child pornography";
- the limitations of our current privacy laws and the dire implications these have for law enforcement agencies working to find offenders and rescue child victims;
- the importance of devoting more resources to identifying and rescuing the children found in sexual abuse images;
- the need to better understand and address the needs of children who have been identified as victims of Internet-facilitated sexual abuse; and
- solutions for reducing the distribution of child sexual abuse images.

The recommendations contained in this report are directed to the Ministers of Justice and Public Safety, the National Child Exploitation Coordination Centre of the RCMP and the Policy Centre for Victim Issues of the Department of Justice.

[1] Gregory Bonnell, "Man who sexually abused daughter live on internet sentenced to five years," Canadian Press, December 20, 2007.



GENERALLY, MORE THAN 90 PERCENT OF CANADIANS are concerned about the distribution of child sexual abuse images, and child sexual exploitation is ranked as one of the top three concerns for parents regarding children.[3] The number of charges for production or distribution of child pornography increased by 900 percent between 1998 and 2003.[4]

Despite these clear concerns, the issue of child sexual abuse and the Internet can sometimes seem to be as difficult to discuss as to tackle. Unfortunately, we do not have a choice. We cannot afford to turn our heads or cover our ears because the problem is growing. And it is getting exponentially worse. Images are getting more and more violent, and the children in those images are getting younger and younger.

This report provides an overview of child sexual abuse and the Internet; where we are, where we have been, the gaps that exist and what we must do to address them. Specifically, the report provides a summary of the scope of the problem, a brief history of the progress that has been made so far and, most importantly, makes nine recommendations for future changes relating to child

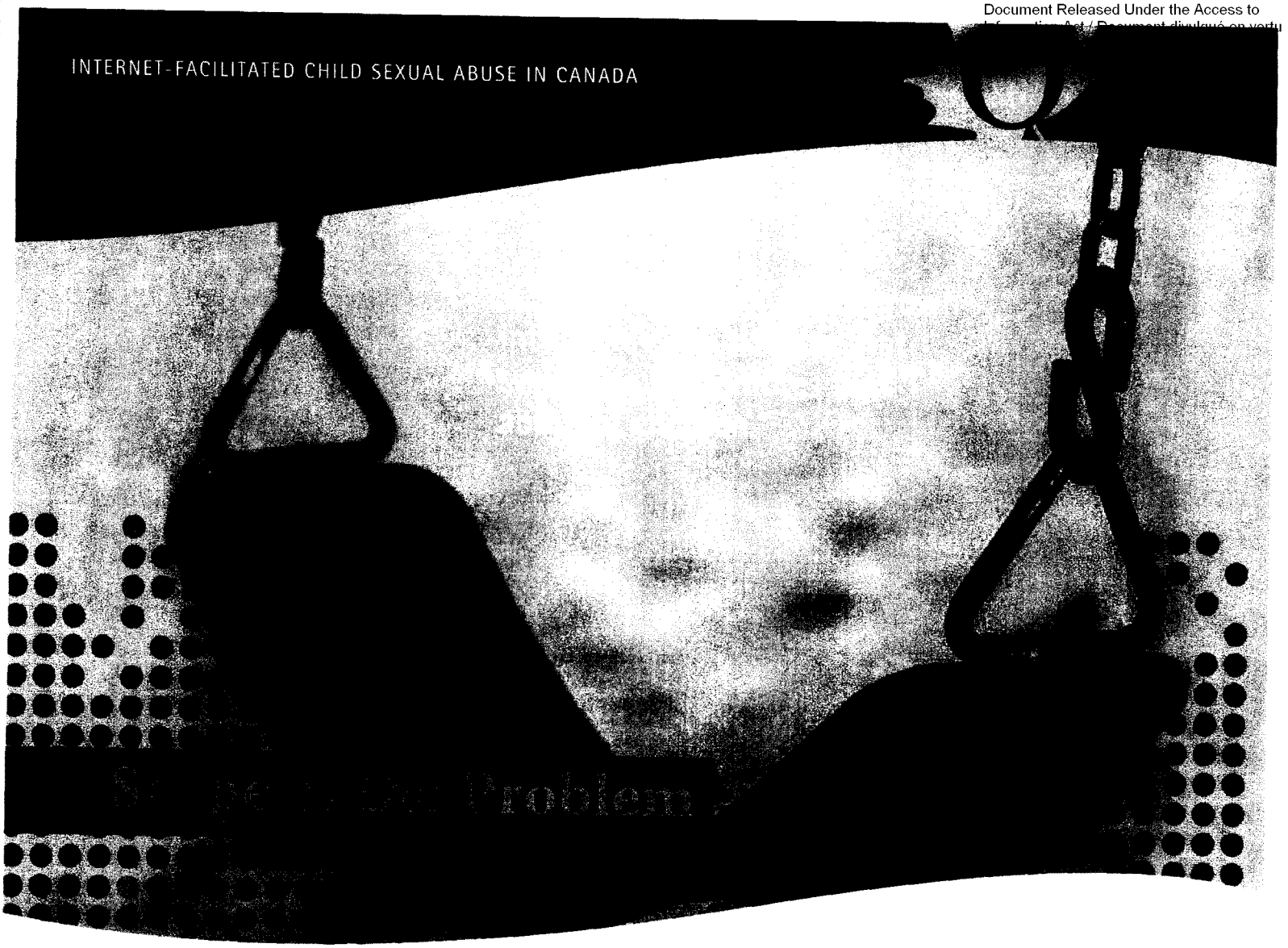
[2] G8 Justice and Home Affairs Ministers, "Reinforcing the International Fight Against Child Pornography," May 24, 2007. www.canadainternational.gc.ca/g8/ministerials-ministerielles/2007/child_porno-enfant_porno.aspx?lang=eng.
[3] Canadian Centre for Child Protection, "What we know," www.protectchildren.ca/app/en/whatwek, March 25, 2008.
[4] Only 33 percent of those convicted of distribution were sentenced to prison (52 percent received probation). Child and Youth as Victims of Crime, *Juristat*, 1, April 20, 2005, p. 11. Statistics Canada Catalogue No. 85-002-XIE.

sexual abuse images, or "child pornography," to the Ministers of Justice and Public Safety, the National Child Exploitation Coordination Centre (NCECC) of the RCMP and the Policy Centre for Victim Issues of the Department of Justice.

These recommendations touch on the term "child pornography" itself, on the limitations of our current privacy laws and the dire implications they have for child victims, on the importance of devoting more resources to identifying and rescuing children who are abused, on properly handling victims who are identified and helping them to heal, and on the need to stop the dissemination of this horrible material.

These recommendations are consistent with the Government of Canada's responsibilities to victims as set out in the *Canadian Statement of Basic Principles of Justice for Victims of Crime*, the *Canadian Charter of Rights and Freedoms* and the various commitments the Government has made at the United Nations and G8.

If accepted, these recommendations will both make a difference in the lives of innocent children and help make Canada a global leader in trying to identify victims and respond to their needs.



Impact of the Internet

"The Internet is not 'creating a sexual interest in children' but it's creating victims."
–Dr. Peter Collins[6]

"The menace that distribution of child pornography through the internet poses cannot be underestimated. The internet provides an unregulated, instant world-wide distribution network that is immediately accessible for viewing, downloading and even wider distribution."[7]

"We were trading pictures...kinda like trading baseball cards. There was also the thrill in collecting them. You wanted to get complete sets so it...was kind of like stamp collecting as well."
–Collector of child pornography[8]

The impact of technology and specifically the Internet on child pornography images cannot be overstated. It can be seen most strikingly in three areas: production, distribution and community. The illusion of anonymity and the near universal accessibility of the Internet enable a vicious cycle: the creation of a community of like-minded individuals

Martin C. Calder, "The Internet: Potential Problem and Pathways to Hands-On Sexual Offending," in Martin C. Calder (ed.), *Child Sexual Abuse and the Internet: Tackling the New Frontier*, 2004.

Alison Haines, "Child porn, pedophilia linked but potential offenders hard to pinpoint," Canwest News Service, March 26, 2006.

R. v Hunt (2002) AJ No. 831 at para. 29 (C.A.).

Ethel Quayle and Ma Taylor, "Child Pornography and the Internet," (2002) 23 *Deviant Behaviour* at 342.

Fast Facts

- Commercial child pornography is estimated to be a *multi-billion* dollar industry worldwide.[9]
- There are over 750,000 pedophiles online at any given time.[10]
- Thousands of new images or videos are put on the Internet every week[11] and hundreds of thousands of searches for child sexual abuse images are performed daily.[12]
- Offenders may have collections of over a million child sexual abuse images.
- An image of a 4-year-old girl in diapers has been shared an estimated 800,000 times.[13]
- Most child sexual abuse image producers are known to the victims:
  - 37 percent are family members.[14]
  - 36 percent are acquaintances.[15]
  - Over 30 percent of those convicted of possessing child pornography were living with minor children; almost 50 percent had access to minors at home, socially or as part of their jobs.[16]

who share and "collect" images, the eventual desire of those individuals to obtain higher numbers of more shocking images and finally, the willingness of members to create more violent images. Once completed, the cycle begins again. Currently, an estimated 500,000 individuals are actively involved in the trafficking of child sexual abuse images on the Internet.[17]

Since the creation of the Internet, the volume of child sexual abuse images has grown exponentially. Images and videos are traded like baseball cards every minute of every day, and the sheer volume is staggering. It is estimated that there are over 5 million unique child sexual abuse images on the Internet.[18]

9 Jonah Rimer, *Literature Review—Responding to Child & Youth Victims of Sexual Exploitation on the Internet*, 2007. The creation and distribution of most images is not related to commercial purposes. www.boostforkids.org/pdf/RCE-Literature-Review.pdf, p. 30.

10 Jane Sims, "So savvy...but so vulnerable," *The Ottawa Sun*, October 12, 2008.

11 Dr. Roberta Sinclair, The National Child Exploitation Coordination Centre, "Internet Facilitated Sexual Exploitation," PowerPoint presentation made to the 2007 National Crime Victim Awareness Week Symposium, April 23, 2007.

12 Ibid.

13 Suzanne Fournier, "Police outgunned by Internet perverts," *Vancouver Province*, October 22, 2008.

14 Jonah Rimer, *Literature Review—Responding to Child & Youth Victims of Sexual Exploitation on the Internet*, 2007, p. 25.

15 Ibid.

16 Adrian Humphreys, "Predators among us—do we have an epidemic or not?," *National Post*, October 20, 2007. These statistics refer to a study done by the National Center for Missing and Exploited Children regarding 1,713 people charged with possessing child pornography.

17 "President Bush signs child protection bill into law," October 14, 2008. /cbs4.com/seenon/internet.sex.predator.2.840236.html.

18 Dr. Michael Bourke, "Child Pornography and Hands-on Abuse," Dallas Crimes Against Children Conference, August 12, 2008.

User as abuser

"...they trade them just like hockey cards. Just like a sports fan would try to collect an entire team in a sport, they will try to collect all 20 images of this young girl. It's called a series."
–OPP Detective Paul Schambers[19]

On May 12, 2003, 10-year-old Holly Jones was abducted while walking home from a friend's house. Minutes before he forced her into his home, sexually assaulted and murdered her, Michael Briere was looking at child sexual abuse images online.

Briere pled guilty to first degree murder and is currently serving a life sentence. At his sentencing hearing, Briere told the court he was consumed by desire after viewing child pornography and that, "Viewing the material does motivate you to do other things. The more I saw it, the more I longed for it in my heart.... I really wanted to have sex with a child. And that was all-consuming."[20]

Everyone who knowingly views and accesses child sexual abuse images for gratification purposes is an abuser. Whether it is the very act of degrading that child by viewing the image, or the niche market that viewers create for those producing the material, or the hands-on abuse inflicted by the offenders themselves, in each case a child is being abused.

The creation and distribution of most images is generally not motivated by commercial purposes. Some abusers take photographs so they can use them for sexual gratification in the future. Others use these sexually abusive images to groom children for future abuse or to coerce their child victims into silence. In recent years, a growing number of offenders indicated that they were motivated to produce these vile images to enhance their status with other child abusers on the Internet.[21]

There are those who may argue that viewers are "just looking at pictures." However, research suggests it is not that simple. In *R. v. Sharpe*, Chief Justice McLachlin of the Supreme Court of Canada stated that "the link between the production of child pornography and harm to children is very strong."[22] According to Jonah Rimer, research assistant with the BOOST Child Abuse Prevention & Intervention Centre, more than half of child pornography offenders either abuse or attempt to abuse children.[23]

Child pornography offenders average 20 victims each—more than double that of contact offenders.[24]

19 Tracy McLaughlin, "Kid-sex pics traded like hockey cards: Cop," *Toronto Sun*, September 22, 2008.
20 Julian Sher, *Caught in the Web: Inside the Police Hunt to Rescue Children from Online Predators*, Perseus Publishing, 2007, p. 38.
21 Michelle Collins (National Center for Missing and Exploited Children), "Child Pornography: A Closer Look," *Police Chief Magazine*, March 2007, 74(3).
22 R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R. 45, para. 92.
23 Jonah Rimer, *Literature Review—Responding to Child & Youth Victims of Sexual Exploitation on the Internet*, 2007, p. 32.
24 Julian Sher, *Caught in the Web*, 2007, pp. 40–41.

Dr. Michael Bourke and Andres Hernandez (Federal Bureau of Prisons) suggest the numbers may be even higher than 50 percent. Their study, which looked at prisoners serving sentences for child pornography offences (as opposed to contact offences), found that child pornography offenders had in fact molested thousands of children, none of whom had reported the abuse.

"The dramatic increase (2,369%) in the number of contact sexual offences acknowledged by the treatment participants challenges the often-repeated assertion that child pornography offenders are only involved with pictures. It appears that these offenders are far from being innocent, sexually curious men who, through naiveté or dumb luck, became entangled in the World Wide Web...."[25]

The study found that less than 2 percent of subjects who entered treatment without known hands-on offences were verified to be "just looking at pictures." Instead, 85 percent of the sample admitted to being child abusers which, as the study points out, calls into question whether it is useful to discriminate between child pornographers and child abusers or even pedophiles.[26]

Similarly, a study conducted by Toronto's Centre for Addiction and Mental Health compared men who were convicted of molesting children and others who were convicted of possessing illegal photos. Researchers found that the offenders who were convicted of the possession offences had a higher chance of exhibiting a pedophile attraction to children than men who actually molested children. Dr. Seto wrote, "Our results indicate that child pornography offending is a valid diagnostic indicator of pedophilia.... In fact, child pornography offenders, regardless of whether they had a history of sexual offences against child victims, were more likely to show a pedophilic pattern of sexual arousal than were a combined group of offenders against children."[27]

Finally, while the reasons behind the abuse may not be clear, some suggest that the desire for new pictures can "lead some consumers to abuse their own, or neighbouring children, in order to supply fresh images for barter or sale."[28]

25 Dr. Michael Bourke and Andres Hernandez, "The Butner Study Redux: A Report of the Incidence of Hands-On Child Victimization by Child Pornography Offenders," (in press), pp. 17–18. There is some ongoing debate about this study.

26 Ibid., p. 18.

27 Dr. Michael Seto et al. "Child Pornography Offenses Are Valid Diagnostic Indicator of Pedophilia," *Journal of Abnormal Psychology*, 2006 115(3), p. 613.

28 Susan J. Creighton, "Child pornography: Images of the abuse of children," November 2003. www.nspcc.org.uk.

Younger victims and increasing violence

In addition to their growing number, child sexual abuse images are getting more and more shocking. As Ontario Provincial Police (OPP) Detective Inspector Angie Howe explained to the Senate Legal and Constitutional Affairs Committee, "The images are getting more violent and the children in the photos are getting younger. As recently as one year ago, we did not often see pictures with babies, where now it is normal to see babies in many collections that we find. There is even a highly sought after series on the Internet of a newborn baby being violated. She still has her umbilical cord attached, she is that young."[29]

"Daddy, it hurts. It hurts so bad."

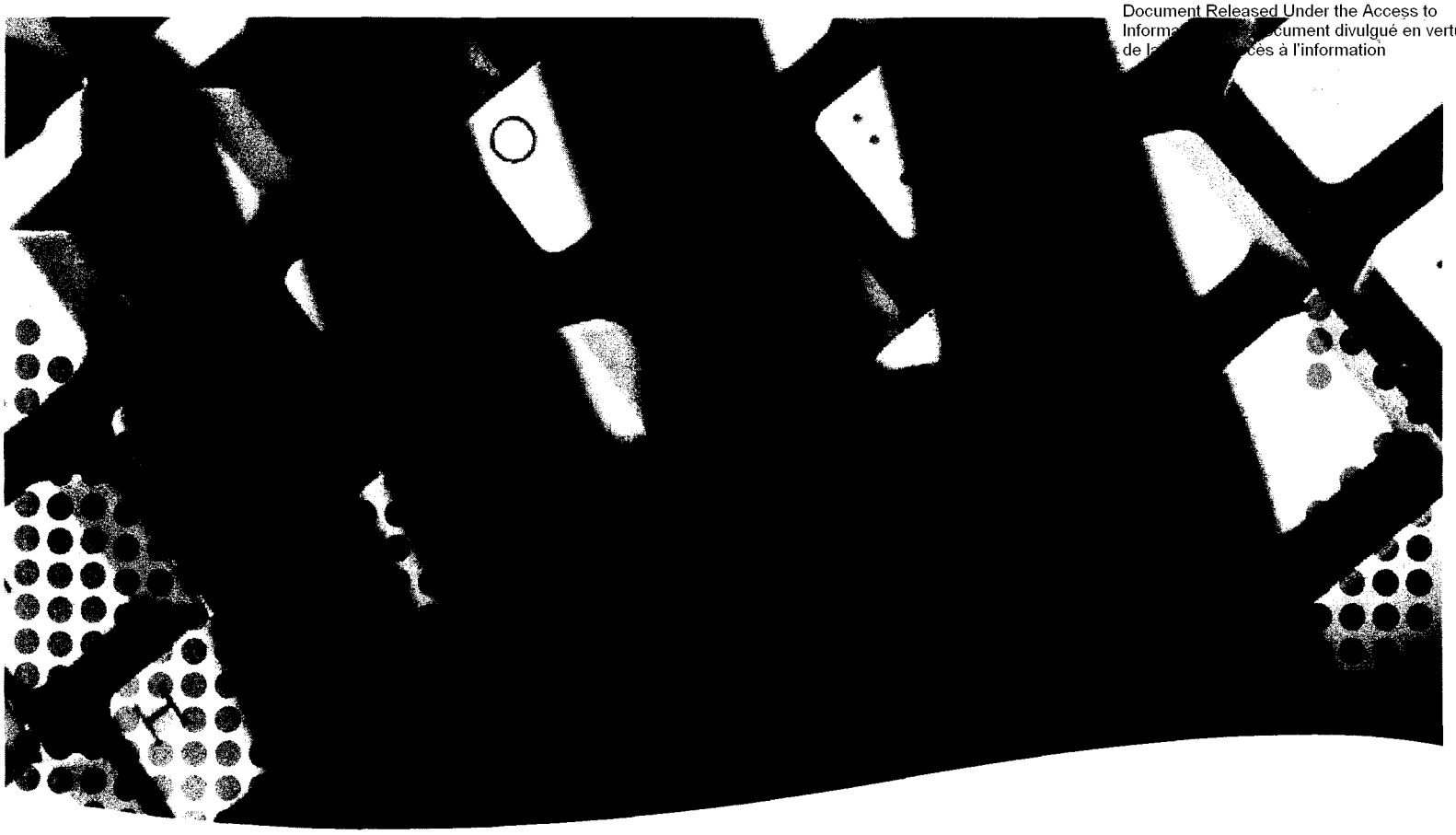
–Audiotape of a young girl as her father abuses her

"Many of the images which I see on a regular basis show severe vaginal and anal assault against toddlers, bondage of these children with gags in their mouths, ligatures around their necks, and on occasion, physical beatings in conjunction with video clips of brutal oral, vaginal and anal penetration."[30]

–Dr. Sharon Cooper, Speech to U.S. Congress in 2006

- Younger children:
  - 83 percent of children are 12 years old or younger.[31]
  - 39 percent had images of children between the ages of 3 and 5.[32]
  - 19 percent had images of infants under 3 years old.[33]
- More violent content:
  - Over 80 percent of the images involve penetration.[34]
  - Over 70 percent show sexual contact between a minor and an adult.[35]
  - 20 percent of the images involve torture or bondage.[36]
  - The number of images of "serious child abuse" has quadrupled between 2003 and 2007.[37]
  - 87 percent had images of prepubescent children that were highly graphic.[38]

[29] OPP Detective Inspector Angie Howe, Senate Legal and Constitutional Affairs Committee, 2005.
[30] Dr. Sharon Cooper, Opening Oral Testimony for the US Senate Committee on Commerce, Science and Transportation, September 19, 2006.
[31] H.R. 4120, *An Act to amend title 18, United States Code, to provide for more effective prosecution of cases involving child pornography, and for other purposes.*
[32] *National Juvenile Online Victimization Study* (NIOV) 2004.
[33] Ibid.
[34] Janis Wolak et al. "Internet Sex Crimes Against Minors: The Response of Law Enforcement," November 2003. www.missingkids.com/en_US/publications/NC132.pdf.
[35] Ibid.
[36] CTV.ca, July 23, 2006.
[37] According to Internet Watch Foundation; Jonah Rimer, *Literature Review—Responding to Child & Youth Victims of Sexual Exploitation on the Internet*, 2007, p. 16.
[38] *Juvenile Online Victimization Incidence Study (JOVIS)* 2004.



Examples of this violence are being seen across Canada. In an Ontario case, a father pled guilty to possessing and accessing child sexual abuse images, which included a five-minute video in which a naked 9-year-old girl is anally, vaginally and orally penetrated and another in which an adult male attempts to penetrate a 6-year-old girl. Police in Winnipeg arrested an American man who had videos of girls between the ages of 4 and 12 performing oral sex on adult men. In Quebec, provincial police arrested several men alleged to be involved in an international child pornography ring that operated over the Internet. The victims of this ring included those of elementary school age and a baby who was just a few months old.[39] Sadly, these examples are not even the worst of the material available.

[39] Peter Rakobowchuk, "Quebec police say baby was part of porn ring," *The Toronto Star*, June 25, 2008.

"Sometimes, you can hear the children cry."

-Paul Gillespie, retired Detective Sergeant, Toronto Police Sex Crime Unit

CANADA'S CURRENT CHILD PORNOGRAPHY LEGISLATION was passed in 1993 and then updated in 2002 to respond to the new reality of the Internet. The update included the creation of the new offence of using the Internet to communicate with a young person for the purpose of facilitating the commission of a sexual offence against that child—commonly known as "child luring."

Two years later, the federal government launched the National Strategy to Protect Children from Sexual Exploitation on the Internet. The strategy included the creation of the Royal Canadian Mounted Police (RCMP) National Child Exploitation Coordination Centre, a clearing house and coordination centre for international requests to conduct investigations in Canada related to child sexual exploitation on the Internet. On February 10, 2009, the Minister of Public Safety announced the renewal of this strategy.

In 2005, Parliament expanded the definition of child pornography, increased the maximum penalty for all child pornography offences and introduced mandatory minimum penalties. That same year, the Manitoba-based organization Cybertip.ca became Canada's national tipline for reporting the online sexual exploitation of children.[40]

[40] www.protectchildren.ca/app/en/.

During this period, Canada took action not just at home, but in the international community, leading our counterparts in learning how to better respond to the abuse of children.

Canada sponsored the United Nations Guidelines on *Justice Matters involving Child Victims and Witnesses of Crime.*[41] Canada was also a signatory to the United Nations *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution, and child pornography* (2000), which requires state parties to protect children from all forms of sexual exploitation and abuse and to take appropriate measures to prevent the exploitative use of children in pornographic performances and materials.

In 2007, Canada's Ministers of Justice and Public Safety joined other G8 Ministers and agreed to accelerate efforts "to ensuring the implementation and effectiveness of our own laws relating to child pornography, and to taking steps to update and improve those laws when necessary and where appropriate."[42] That same year, the Federal/Provincial/Territorial (FPT) Ministers responsible for Justice "expressed serious concern about child pornography on the Internet and asked officials, on a priority basis, to complete their work in examining measures, including legislation, to increase cooperation of Internet Service Providers in assisting law enforcement officials to identify criminals and rescue child victims."[43]

In 2007, the federal government also took further steps to protect children by raising the age of consent from 14 to 16, enhancing the dangerous offender provisions of the *Criminal Code* and dedicating an additional $6 million to the RCMP to protect children "from online sexual exploitation..."[44]

In January 2008, former Public Safety Minister Stockwell Day gave $2 million to the Canadian Centre for Child Protection, which operates Cybertip.ca, declaring it as "another concrete action that our government is taking to protect children from online adult sexual predators, and to prevent them from being sexually abused."[45]

In September 2008, the FPT Ministers responsible for Justice agreed that "Canada's response to child pornography could be enhanced by federal legislation requiring any agency whose services could be used to facilitate the commission of online child pornography offences to report suspected material."[46] This would bring Canada in line with other countries, like the United States and Australia which, under federal law, require Electronic Service Providers (ESPs) to report the discovery of child sexual abuse images. Some provinces, like Manitoba and Ontario, have passed legislation regarding mandatory reporting of child sexual abuse images.

41 Part of the International Labour Organization's *Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour, Convention 182.*

42 G8 Justice and Home Affairs Ministers, May 24, 2007. www.g8.gc.ca/childpornography-en.asp.

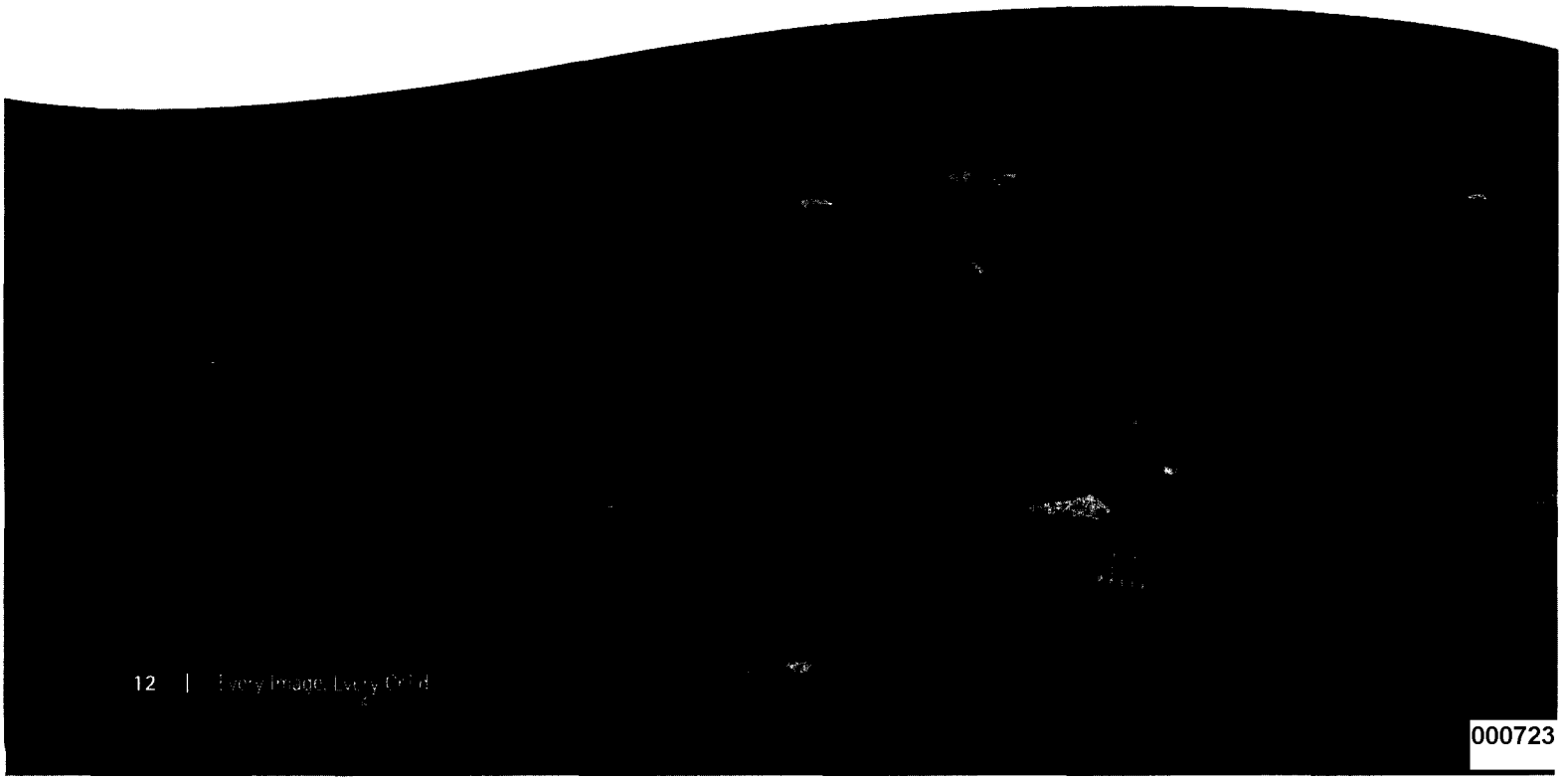
43 Federal-Provincial-Territorial Meeting of Ministers responsible for Justice Meet [news release]. Winnipeg, Manitoba, November 14–16, 2007. www.scics.gc.ca/cinfo07/830926004_e.html.

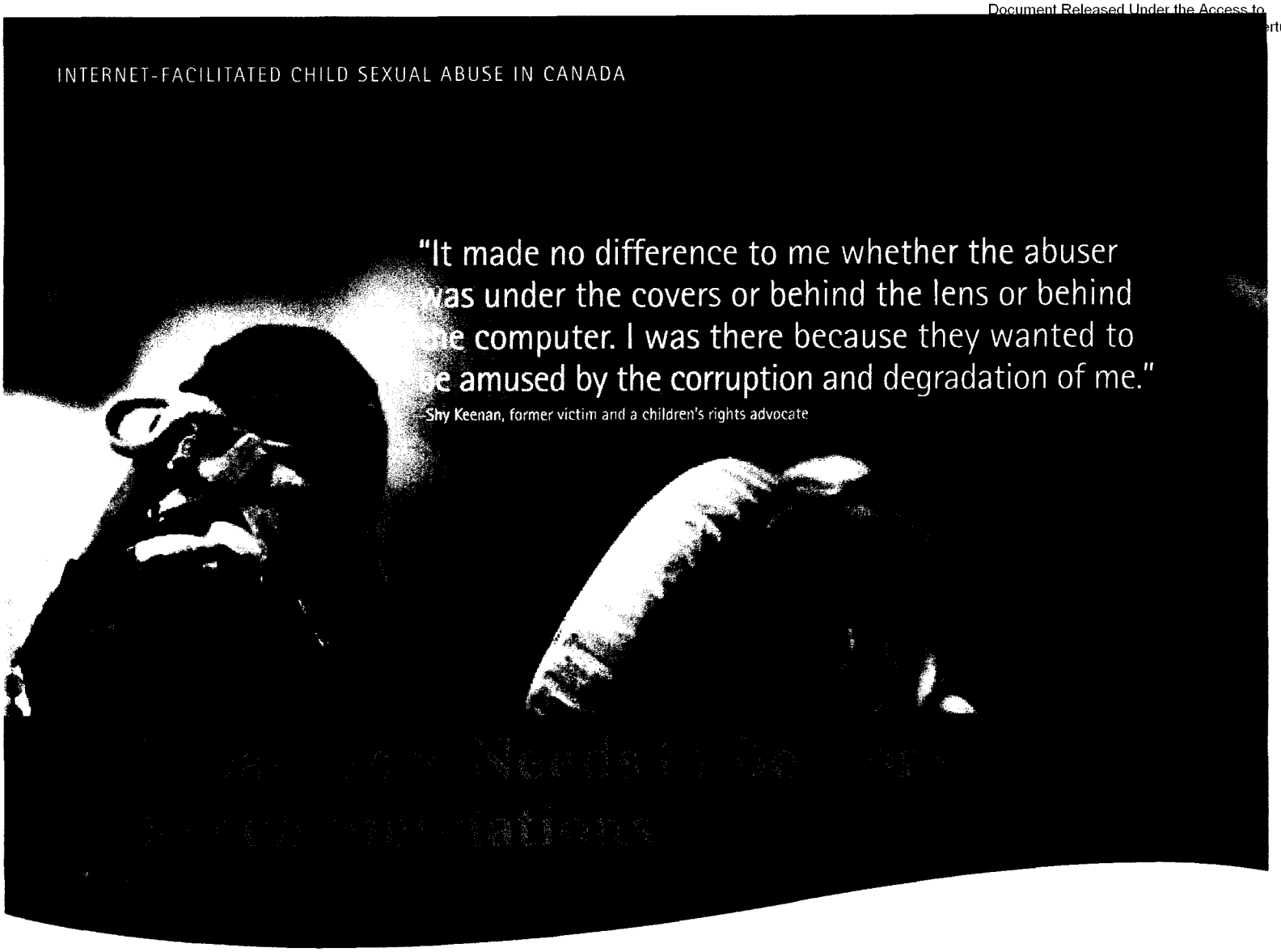
44 The Honourable Jim Flaherty, 2007 Budget Speech, March 19, 2007. http://www.budget.gc.ca/2007/speech-discours/speech-discours-eng.html.

45 www.publicsafety.gc.ca/media/nr/2008/nr20080129-eng.aspx.

46 September 5, 2008. http://canada.justice.gc.ca/eng/news-nouv/nr-cp/2008/doc_32302.html.

We encourage the Government to proceed with legislation that would require not only ISPs, but social networking sites, computer repair shops and Internet content hosts to report suspected child pornography. However, this must be part of an overall government strategy to combat this problem. Mandatory reporting on its own is not likely to make a significant difference in the fight against online child sexual exploitation. Law enforcement agencies report now that they are struggling to keep up with the number of cases they have. The most serious problem is not lack of reports, but about accessing information about suspects, identifying children and preventing future abuse. The federal government must avoid acting on mandatory reporting just to be seen to be doing something without addressing the priority issues identified in this report.





DESPITE ITS PAST SUCCESSES, CANADA HAS MUCH MORE TO DO.

There are a number of sizable gaps where children are falling through the cracks and offenders are gaining momentum. We must move to address these gaps now, before we fall too far behind.

Specifically, we must be honest about the horror of the situation and address it as such. We need to reconsider which has higher value: an offender's right to anonymity or the real harm being done to children. We need to give authorities the tools they need to identify these children and rescue them and then, once the victims are found, we need to have the resources and expertise in place to properly care for these children and to help them heal. Finally, we need to hold those that share and distribute child sexual abuse images accountable for their role and find meaningful ways to ensure the private sector is part of the solution.

While the issue is enormous, this report presents nine practical and feasible recommendations to address the issue of child sexual exploitation as it pertains to the Internet.

1. CHILD PORNOGRAPHY— A DANGEROUS TERM

To begin, it is important to first address the term "child pornography."

In 2007, in a special report entitled *Reinforcing the International Fight Against Child Pornography*, the G8 Justice and Home Affairs Ministers noted that while the term "child pornography" is used commonly in legislation and international conventions, it "does not appropriately or adequately describe the severe abuse and exploitation of children that is involved in these visual representations."[47]

As the Ministers point out, the real nature of the problem is, in essence, sexually explicit images or representations of children. The term "pornography," however, is commonly understood to be associated with depictions of sexual activity between *consenting* individuals. Children cannot consent to sexual relations. For this reason, use of the term "child pornography" mischaracterizes sexual representations where children are involved. The term does not properly convey the real harm that is experienced by young victims and the seriousness of the activities of those persons who sexually exploit children in this way. "This misunderstanding compromises the effectiveness of our very important efforts to protect children from this form of sexual exploitation."[48]

This applies to other similar terms, such as "kiddie porn" or "child porn," which may also contribute to the public misperception about what law enforcement is finding on the Internet. As Jim Gamble, Chief of the Child Exploitation and Online Protection Centre, points out, "If a woman is raped and her attacker makes a video of it, no one would dare suggest the video was adult pornography. He is a rapist, not a pornographer."[49]

For this reason, this report uses the term "child sexual abuse images." We will use the term "child pornography" only when making specific reference to the *Criminal Code of Canada* or the laws of other countries, as there is no internationally agreed-upon term at this time.[50] While no words can adequately convey the horror these children are suffering, we believe the term "child sexual abuse images" (or videos) more accurately describes that harsh reality than "child pornography." Based on this, we recommend that legislation be amended to better distinguish child sexual abuse images from the adult, legally based commercial industry.

RECOMMENDATION 1—That the federal government introduce legislation to amend the child pornography provisions in the *Criminal Code* to provide a more accurate description of the crime (i.e. such as child sexual abuse images, child sexual abuse videos, child sexual abuse writings) to ensure a more accurate reflection of the harm that is done to victims.

---

47 www.virtualglobaltaskforce.com/news/G8Statement.pdf

48 www.canadainternational.gc.ca/g8/ministerials-ministerielles/2007/child_porno-enfant_porno.aspx?lang=eng.

49 The U.K. created the Child Exploitation and Online Protection (CEOP) Centre to play a decisive role in partnership with the Department for Children, Schools and Families (DCSF), police forces, offender managers, children's services and other stakeholders in the protection of children, young people, families and society from pedophiles and sex offenders—particularly those who use the Internet. The CEOP Centre works across the U.K. and uses international links to combine police powers with the expertise of children's charities, business sectors, government and other interested organizations all focused on tackling child sex abuse wherever it happens.

50 In Queensland, the term used is "child exploitation material." CRIMINAL CODE 1899 - SECT 207A.

2. RESCUING CHILDREN FROM INTERNET-FACILITATED SEXUAL ABUSE

The key step in rescuing victims of abuse is to identify and locate them. While this may seem a daunting task, ironically the same Internet technology that facilitates the repeated victimization of children can help law enforcement identify and rescue those same victims.

One of the most powerful clues that police have available to assist them in this regard is the Internet Protocol or "IP" address.

An IP address is a numerical identifier given to a particular computer or device when it is hooked up to the Internet—something like a licence plate for a car. When offenders are exchanging images, the IP address is often publicly accessible. This information can often help authorities to determine the location of the offender by providing more information about the Internet Service Provider (ISP) the offender is using (i.e. the company that is providing the abuser with Internet access) as well as the geographic region of the user.

In some cases, the IP address can actually narrow down the location of the abuser to a specific city. Once a geographic area is defined, the next step is to contact the ISP and to ask for the name and address of the customer registered to that IP address.

Unfortunately in Canada, this is where authorities sometimes hit a dead end and the investigation is forced to shut down. According to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), ISPs in Canada "may," but are not legally obliged to, provide police with information such as the name and address of customers who are known to be exchanging or distributing child sexual abuse images.

Currently, police send a standard letter to the ISP, which asks for customer name and address information for a specific IP address and for a specific date and time.[51] Whether or not the ISP provides this information is up to the individual company. Many ISPs have provisions in their service agreement that say they will disclose *any information* they, in their sole discretion, deem necessary to satisfy any applicable law, regulation, legal process, or government request.[52] The *Bell Code of Fair Information Practices* defines "personal information" for a customer as "a customer's credit information, billing records, service and equipment, and any recorded complaints."[53] Basic subscriber information such as the customer's name and address is *not* considered personal information for the purposes of the Privacy Policy.

Even though many ISPs do cooperate, 30 to 40 percent of requests are still denied.[54] Some ISPs are hesitant to cooperate for fear of resulting legal action by customers, whereas others even go so far as to advertise their lack of cooperation with police to attract customers.[55]

When it comes to protecting our children, depending on the goodwill of any industry is not good enough.

[51] The letter was developed by the Canadian Coalition Against Child Exploitation (CCAICE), a voluntary group of partners that work to reduce child sexual exploitation on the Internet. CCAICE includes industry, government, non-governmental and law enforcement stakeholders from across the country. The existing arrangement is based on paragraph 7(3)(c) of the *Personal Information Protection and Electronic Documents Act*.

[52] Bell *Customer Service Agreement*, p. 14.

[53] Bell *Code of Fair Information Practices*, Definitions, p. 4.

[54] NCECC Submission to Public Safety Canada, "Customer Name and Address Information Consultation," October 2007.

[55] Ibid., p. 4.

Giving authorities the tools they need

The idea of requiring ISPs to provide customer name and address information is not new. For years, the law enforcement community has been calling for legislative reforms to require ISPs to provide this information without judicial authorization (i.e. a warrant).[56]

The same sentiments were expressed in 2007 when the Office of the Federal Ombudsman for Victims of Crime brought together law enforcement experts from across Canada for a roundtable on Internet-facilitated child sexual abuse. Without exception, the number one barrier to pursuing cases identified by law enforcement attending the roundtable was the lack of access to customer name and address information.

The RCMP's National Child Exploitation Coordination Centre (NCECC) warns, "As long as they [ISPs] are at liberty to decline to provide this information to police upon request, investigations can and are being impaired. In the case of online child exploitation matters, *the result is that many investigations cannot proceed* (emphasis added)."[57]

A 2007 Department of Public Safety consultation document on customer name and address information provided a similar warning: "If the custodian of the information is not cooperative when a request for such information is made, law enforcement agencies may have no means to compel the production of information pertaining to the customer.... *The availability of such building-block information is often the difference between the start and finish of an investigation* (emphasis added)."[58]

Sadly, this challenge translates into unsuccessful rescue efforts. In one case, an online undercover officer investigating the live online sexual abuse of a child on a Friday evening requested the customer name and

[56] A recent report prepared by Deloitte for the Canadian Association of Police Boards, entitled *Report on Cybercrime in Canada* (April 25, 2008, pp. 1–2), which included interviews with law enforcement, Crowns and others with experience in this area, said there was support for changes to existing legislation that would enable information sharing with law enforcement agencies, with lower judicial standards than those now applied to search and seizure warrant and mandatory reporting requirements for child pornography.

[57] NCECC Submission to Public Safety Canada, "Customer Name and Address Information Consultation," October 2007.

[58] www.publicsafety.gc.ca/prg/ns/cna-en.asp. The document also clarified "the possible scope of CNA information to be obtained is later identified, but *it should be noted from the outset that it would not, in any formulation, include the content of communications or the Web sites an individual visited while online....*"

address information from the ISP but was told to call back on Monday during regular business hours.[59] In June 2007, a law enforcement agency asked an ISP for customer information because it had reason to believe children were at risk. The ISP refused to provide the information unless the investigator produced judicial authorization. It was not until pressure was applied by Child Welfare Services that the ISP finally provided the customer's name. By this time, the suspect had moved and dismantled his computer.

In a few cases, police have been able to convince ISPs of the importance of the information by going to extreme lengths. Such was the case when an officer investigating live sexual abuse was told by the ISP to get judicial authorization. The ISP became cooperative only after the officer held the phone to the computer speakers to let the representative hear the child's screams.

The right to privacy

"We recognize that privacy is an important value underlying the right to be free from unreasonable search and seizure and the right to liberty. However, the privacy of those who possess child pornography is not the only interest at stake in this appeal. The privacy interests of those children...are engaged by the fact that a permanent record of their sexual exploitation is produced."

–Madam Justice L'Heureux-Dubé[60]

Any public policy debate that involves the Internet must include the issue of privacy and the very real and legitimate privacy concerns that Canadians have.

The public is rightly concerned about their privacy and has a right to be protected from unreasonable search and seizure. As such, privacy should be considered when deciding what kinds of information law enforcement should have access to regarding Internet customers. Efforts to address enforcement issues to date, however, have been too narrowly focused on false warnings of "Big Brother" or have fostered misconceptions about what kind of information police are able to obtain with an IP address and a customer's name and address. Very little attention has been given to the real, and more serious, privacy interests of the children whose images of abuse and torture are being traded.

Unfortunately, Canadians have been misled about the potential privacy implications of legislation that would permit law enforcement access to customer name and address (CNA) information. For example, one privacy advocate contends, "CNA information, like name and address, are keys to acquiring other personal information, including highly sensitive data such as health or financial records."[61] The author goes on to argue that "...the government is in fact seeking enhanced search powers through expedited processes and lower standards, thereby slashing privacy safeguards and expectations."[62] Another said, in response to an Ontario Superior Court decision that upheld police access to CNA information without a warrant,[63] "It is not just your name. It is your whole Internet surfing history."[64]

59 Ibid., p. 5.
60 *R. v. Sharpe*, 2001 SCC 2, [2001] 1 S.C.R. 45, para. 189.
61 Ian Kerr, Submission to the Customer Name and Address Consultation, October 19, 2007. www.idtrail.org/content/view/763/42/.
62 Ibid.
63 *R. v. Wilson*, ONCJ St-Thomas, no. 4191/08, February 10, 2009.
64 Shannon Kari, "Judge's ruling could let police access IP data without warrant," *Ottawa Citizen*, February 13, 2009.

These points touch on the two most common arguments put forward by privacy advocates:

1. It is inappropriate for law enforcement to seek, without judicial authority, the name and address of a potential offender.
2. Providing customer and name and address information gives police enhanced powers to review and collect more personal information, such as health records or a client's Internet surfing history.

These points are false and confuse the issue by offering dangerous misconceptions. First, a person's name and address are not private and law enforcement does not need judicial authorization to obtain them. Second, if police want more information about a suspect, such as his or her Internet surfing history or medical records, they must obtain judicial authorization.

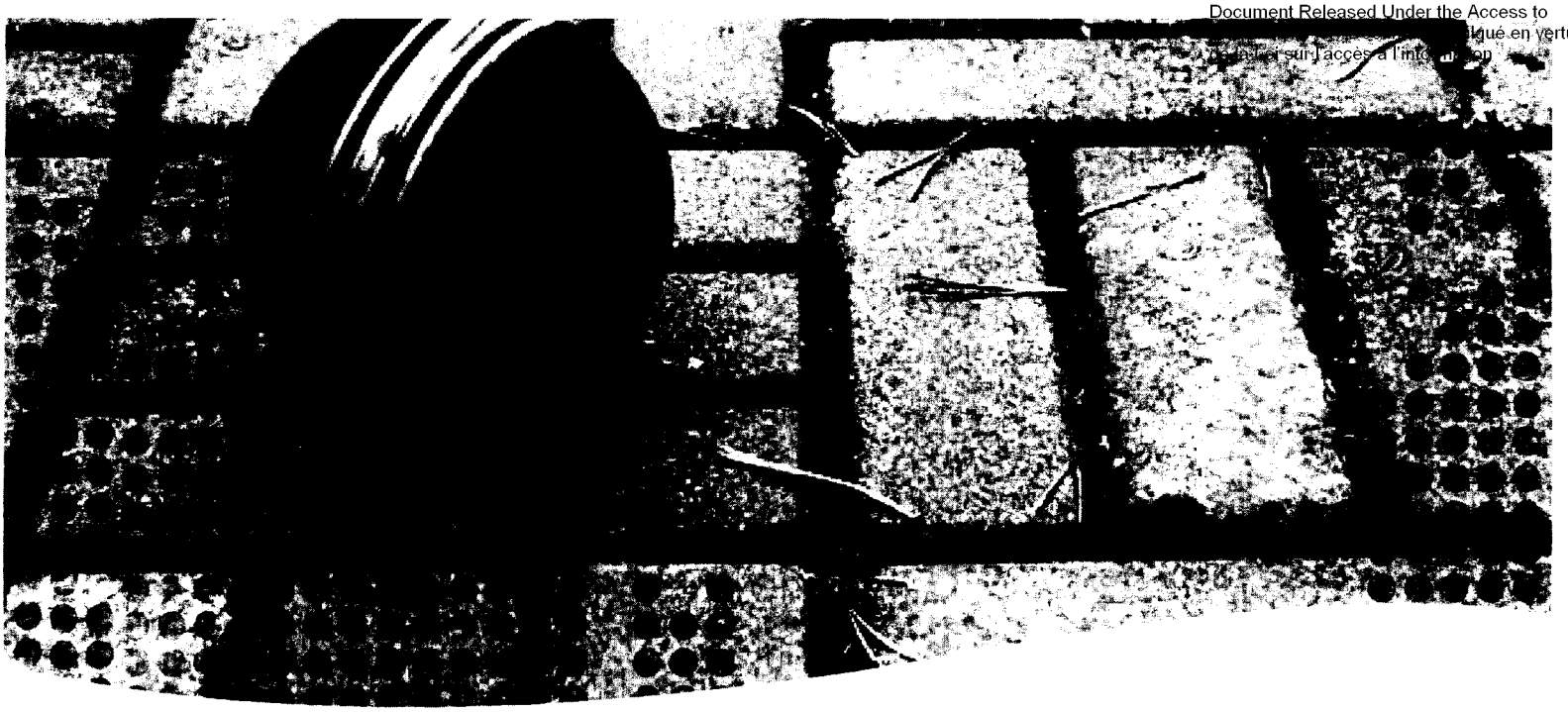
In *R. v. Plant*, the Supreme Court of Canada said that for information to be constitutionally protected, it must be at the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state, and that the information must disclose 'intimate details' about the 'personal lifestyle or private decisions.'"[65]

The *Plant* case involved a police investigation into a marijuana grow-op. The police obtained information from the electricity company—another service provider—regarding the owner's electricity use. They used this information to obtain a search warrant. The Supreme Court said:

"The police check of computerized records was not unreasonable.... In view of the nature of the information, the relationship between the accused and the electrical utility, the place and manner of the search and the seriousness of the offence under investigation, it cannot be concluded that the accused held a reasonable expectation of privacy in relation to the computerized electricity records which outweighed the state interest in enforcing the laws relating to narcotics offences. While they reveal the pattern of electricity consumption in the residence, the records do not reveal intimate details of the accused's life. Since the search does not fall within the parameters of s. 8 of the *Charter*, this information was available to the police to support the application for a search warrant."[66]

In *R. v. David Ward*, Justice Lalonde said, "There is certainly no evidence...that disclosure of the applicant's name and address only, absent the police obtaining a search warrant, would open the floodgates to intimate personal details about the applicant's lifestyle, habits and choices."[67]

65 *R. v. Plant*, [1993] 3 S.C.R. 281.
66 Ibid.
67 *R. v. David Ward*, Sudbury Court File No. 071751, June 16 and 17, 2008.



In February 2009, Justice Lynne Leitch of the Ontario Superior Court ruled "[t]here is no reasonable expectation of privacy in the information provided by Bell considering the nature of that information. One's name and address... are not biographical information one expects would be kept private from the state. It is information available in a public directory...."[68] This marked the first time a Superior Court had issued such a ruling, although some lower courts have made consistent rulings.[69]

In *R. v. Quinn*, at the request of law enforcement, a bank confirmed that a specific account belonged to the appellant. This information was later used to obtain a search warrant.[70] The British Columbia Court of Appeal upheld the warrant and finding saying, "*[T]here was no search, much less any unreasonable search as envisioned in the Charter.*"[71]

Obtaining a suspect's name and address is already common practice during an investigation. Police get access to an individual's name and address in a variety of ways. If they pull your car over, you must show them your licence. If you are seen driving away from an accident, they can access your information through your licence plate.

[68] *R. v. Wilson*, ONCJ St-Thomas, no. 4191/08, February 10, 2009.
[69] Ibid. Most decisions support the principles that a customer's name and address are not "private" information, but there have been dissenting opinions (*R. v. Kwok*).
[70] *R. v. Quinn* 2006 BCCA 255.
[71] Ibid., para. 93.

The federal government already authorizes agencies the power to collect this type of information without a warrant. For example, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), which works to identify money laundering and terrorist activities financing, can request information such as business records, and enter business premises, without a warrant.[72] The information must be kept in such a way as to enable FINTRAC access in a timely fashion and failure to comply with these requirements could lead to imprisonment for up to five years.

Certain ISPs will only provide CNA information without a warrant in cases where "imminent" danger is identified. Some ISPs have agreed to provide the information upon request only if someone is in imminent danger. However, if police cannot prove imminent danger the ISPs will usually require judicial authorization.[73]

This is problematic for a number of reasons, including the fact that imminent danger is not always obvious. In 2006, police in Aylmer, Quebec, arrested a 19-year-old man after he sent child sexual abuse images to an undercover Ottawa police officer online. After the arrest, the man admitted to sexually abusing his 8-month-old son and filming it. At the time of his arrest, the police had no idea he was abusing his son.[74] In this scenario, because police could not have known or demonstrated in advance that a child was in imminent danger, a little boy would have gone on being abused. Similarly, in February 2009, law enforcement in Ontario arrested over 30 men during a province-wide child pornography sweep. A 12-year-old girl was removed from the home of one of the men arrested on suspicion of distributing child sexual abuse images, but at the time of his arrest, law enforcement had no reason to believe the man was abusing a child. Clearly, it is not possible for ISPs to determine the level of risk to a child in these situations.

If imminent danger cannot be proven and law enforcement is required to get a warrant, there is a greater risk to the child. First, warrants take time and law enforcement may not be able to get one in time to rescue the child in danger. The more time police spend trying to get judicial authorization for information that is not personal or private, the less time they have available to identify and rescue children. As stated by the Public Safety Minister, "In some of these cases, time is of the essence. If you find a situation where a child is being exploited live online at that time...police services have had good cooperation with a lot of internet service providers, but there are some that aren't so cooperative." [75]

Second, a warrant cannot be obtained in the investigation of a criminal offence until sufficient information "to support reasonable and probable grounds for that offence exists."[76] Obtaining basic CNA information is part of the information that would assist in obtaining a warrant.

Privacy rights of the victim

A balanced discussion of privacy must also consider the rights of the victim.

For victims whose abuse has been shared on the Internet, there is no privacy. They must grow up knowing these images or videos will be on the Internet for the rest of their life. It is a privacy violation that never ends.

72 FINTRAC gets its authority from the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act.*
73 CBC News, "Search warrants for child porn too slow, say RCMP," April 2, 2008. www.cbc.ca/canada/prine-edward-island/story/2008/04/02/childporn-warrants.html.
74 CBCNews.ca, "Quebec man jailed for molesting infant son, making child porn," July 20, 2007.
75 Bill Curry, "New law to give police access to online exchanges," *The Globe and Mail*, February 12, 2009.
76 NCECC Submission to Public Safety, "Customer Name and Address Information Consultation," October 2007, p. 7.

Privacy rights are established in the *Canadian Charter of Rights and Freedoms* and international forums. For example, section 7 of the Charter guarantees the right to life, liberty and security of the person, which is certainly undermined by child pornography.[77] Privacy is also one of the principles the federal government is required to consider under the *Canadian Statement of Basic Principles of Justice for Victims of Crime*. The United Nations Resolution on Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime also affirms that children have a right to privacy and it should be protected as a matter of primary importance.

In the case of child sexual abuse images, the invasion of privacy goes far beyond simply sharing personal information. Madam Justice L'Heureux-Dubé wrote, "If disseminated, child pornography involving real people immediately violates the privacy rights of those depicted, causing them additional humiliation."[78] She went on to say, "The law intrudes into the private sphere because doing so is necessary to achieve its salutary objectives. The privacy interest restricted by the law is closely related to the specific harmful effects of child pornography. Moreover, the provision's beneficial effects in protecting the privacy interests of children are proportional to the detrimental effects on the privacy of those who possess child pornography."[79]

Two recent decisions have caused some concern about the willingness of the court to consider the privacy interests of the child victim.

The first case involved an artist (Katigbak) who had over 500 images and 30 video clips that constituted child pornography. He claimed he was working on an artistic project (over a six-year period of time) to raise awareness of the effect of child pornography or sexual abuse on the children.[80] The other case (Sauve) involved a manager of a group home where some clients had pedophilic tendencies; he claimed he collected images to help treat a client.[81]

Both men were acquitted because the Courts accepted the accused's justifications for possessing and collecting the images. Both cases addressed the issue of "undue harm to the child" and found that the actions of neither men put children under the age of 18 at undue risk. In Katigbak, the Court relied on the fact that the accused did not purchase the images, he was not sexually motivated and did not intend to distribute them. The Court said this "negatives the concern that the victims are being re-victimized by a viewing of the images."[82] In Sauve, the Court said Parliament was not referring to a general risk of harm to children.

Neither Court, nor the two accused, considered the harm done to the children whose images were being collected. No matter the reason behind it, these children gave no permission to either man to access or collect their images. In doing so, these men contributed to the victims' ongoing abuse.

77 *R. v. Sharpe*, 2001 SCC 2, [2001] 1 S.C.R. 45, para. 189.
78 Ibid., para. 135.
79 Ibid., para. 240.
80 *R. v. Katigbak* (2008) Reasons for Decision. Some of the alleged offences were committed before the 2005 amendment and prior to that the *Criminal Code* referred to "artistic merit or an educational, scientific or medical purpose."
81 *R. v. Sauve* (2008) O.J. No. 4230.
82 *R. v. Katigbak* (2008) Reasons for Decision, para. 36.

The Crown is appealing the Katigbak decision. We urge the Department of Justice to monitor these cases to determine if an amendment is necessary to highlight the privacy interests of the children whose images are being collected.

As a final point, it is important to consider the following: The more time police spend trying to get judicial authorization for information that is not personal or private, the less time they have available to identify and rescue children.

The need for legislative change

The RCMP's NCECC says "the single most important challenge facing investigators of Internet facilitated child exploitation ahead of all other issues, has been their inability to obtain basic customer information such as someone's name and address from Internet Service Providers (ISPs)."[83]

This was confirmed in 2007 when our office held a roundtable with law enforcement from across the country. At the roundtable, law enforcement identified its inability to acquire customer name and address information as the single biggest obstacle to identifying offenders and rescuing child victims of Internet-facilitated child sexual abuse.

In 2006, the Standing Committee on Access to Information, Privacy and Ethics conducted a review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). It heard from victims' groups and law enforcement that, although PIPEDA authorizes ISPs to provide basic information to law enforcement, many were not doing so. Clayton Pecknold of the Canadian Association of Chiefs of Police explained the challenges the police face:

"...we are increasingly seeing some companies interpreting lawful authority to mean that a warrant or court order is required before they comply. This is an interpretation that is not, in our respectful view, consistent with the intent of the drafting of the act. Such an interpretation by companies, while no doubt grounded in a legitimate desire to protect their customers' privacy, is overly restrictive and defeats, in our view, the intent of paragraph 7(3)(*c*.1).[84]

In 2007, the Committee released its fourth report and recommended:

"...that consideration be given to clarifying what is meant by "lawful authority" in section 7(3)(*c*.1) of PIPEDA and that the opening paragraph of section 7(3) be amended to read as follows: 'For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization **shall** disclose personal information without the knowledge or consent of the individual but only if the disclosure is [...].'"

[83] NCECC Submission to Public Safety Canada, "Customer Name and Address Information Consultation," October 2007, p. 1.

[84] Standing Committee on Access to Information, Privacy and Ethics, Meeting 30, February 13, 2007, www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=2695445&Language=E&Mode=1&Parl=39&Ses=1

Responding to the report, the former Minister of Industry confirmed "that the purpose of s.7(3)(*c*.1) is to allow organizations to collaborate with law enforcement and national security agencies without a subpoena, warrant or court order. Organizations who share information with government institutions, including law enforcement and national security agencies, in accordance with the requirements of this provision, are doing so in compliance with PIPEDA."[85]

In October 2007, the Department of Industry released a consultation document on several issues relating to the committee's report, including the proposal to clarify lawful authority. The Office of the Federal Ombudsman for Victims of Crime submitted a written brief to the Minister calling upon him to enact legislation quickly to clarify lawful authority as well as to make a further amendment to the legislation to require ISPs to provide CNA information to police investigating child sexual abuse cases.[86]

In a response sent in November 2007 to the Ombudsman's office, the former Minister of Industry said, "The Government of Canada accords the highest importance to the safety and security of Canadians and recognizes the particularly vulnerable nature of children in the online environment." The former Minister acknowledged that the current law has created "challenges for law enforcement investigations" and that law enforcement reports that its ability to gain access to "basic information that is essential and often quite urgent" has been hindered. He stated that PIPEDA was not intended to be an impediment to the cooperation between companies and law enforcement, yet he said, "Obligations to collaborate in investigations and the establishment of consequences for obstruction currently rest with the *Criminal Code of Canada*. As such, a requirement for compulsory disclosures or information would be incompatible with the purpose of PIPEDA...."[87]

Canada has fallen behind on this point. Other countries, including the U.K., Australia and the U.S., have passed legislation that does not require law enforcement to secure judicial authorization before accessing CNA from an ISP.[88]

In the fall of 2007, the Department of Public Safety released its own consultation document on customer name and address information. The Office of the Federal Ombudsman for Victims of Crime participated in the consultation, urging the former Minister of Public Safety to introduce legislation that would require ISPs to provide CNA information to law enforcement. In response, the Government said it was examining how best to address this serious issue, including the possibility of legislation in this area.[89] On February 11, 2009, the current Minister of Public Safety confirmed he was considering legislation to address problems of enforcing laws in the age of the Internet. Specifically, the Minister stated, "If somebody's engaging in illegal activities on the Internet, whether it be exploitation of children, distributing illegal child pornography, conducting some kind of fraud, simple things like getting username and address should be fairly standard, simple practice. We need to provide police with tools to be able to get that information so that they can carry out these investigations."[90]

RECOMMENDATION 2—That the federal government expedite legislation to require ISPs to provide customer name and address information to law enforcement.

85 Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics, Statutory Review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). www.ic.gc.ca/eic/site/ic1.nsf/eng/h_02861.html.

86 www.victimsfirst.gc.ca.

87 Letter from the Honourable Jim Prentice, Minister of Industry, November 29, 2007.

88 The scheme set out in Bill C-74 and the department's consultation appear to be more restrictive than that of the other three countries. Dominique Valiquet, *Telecommunications and Lawful Access: II. The Legislative Situation in the United States, the United Kingdom and Australia*, February 28, 2006, Library of Parliament. www.parl.gc.ca/information/library/PRBpubs/prb0566-e.html.

89 "Government Response to the Annual Report of the Federal Ombudsman for Victims of Crime, April 2007 to March 2008." http://canada.justice.gc.ca/eng/news-nouv/nr-cp/2009/doc_32330.html.

90 Bill Curry, "New law to give police access to online exchanges," *The Globe and Mail*, February 12, 2009.

3. GATHERING EVIDENCE— DISAPPEARING INFORMATION

As discussed, the ability of police to identify and rescue children in an expedient manner is tied directly to their ability to get information about Internet customers. Obtaining this information, however, is not always straightforward, even with the cooperation of ISPs because in some cases they have already purged it from their systems.

"Client logs" contain information about when a client logged onto the Internet, what the client did while on the Internet and which IP address the session was linked to. This information is very useful for law enforcement agencies that are investigating a case. Police are required to obtain judicial authorization to obtain this information; however, too often even after police have authorization the information is no longer available because it has been erased or purged.

ISPs are not legally obligated to retain client logs. There is also no standard length of time for data retention. In some cases, data are purged after four hours.[91] If the information no longer exists, the investigation cannot proceed. This obviously has serious implications for victims.

The Kids Internet Safety Alliance (KINSA) has called for legislation that requires ISPs to "retain the IP address logs, indicating which subscriber had a particular IP address, for a period of 5 years." KINSA also promotes a requirement that ISPs retain subscriber information for past customers for the same time period.[92]

Data retention requirements would require providers to collect and keep information from all users of a communication service—regardless of whether or not they are the subject of an investigation. This would ensure that information vital to an investigation is not deleted before the police can obtain a search warrant or production order to access the specific data.

[91] NCECC Submission to Public Safety Canada, "Customer Name and Address Information Consultation," October 2007, p. 5.

[92] KINSA was incorporated as the Kids' Internet Safety Association in 2005 and is now known as the Kids' Internet Safety Alliance. KINSA focuses on advocacy, awareness, training and research. www.KINSA.net.

Other countries have data preservation laws that enable law enforcement authorities, during a criminal investigation, to instruct a service provider to set aside specified data about a specific individual or IP address that is already in the service provider's possession until law enforcement procures the proper documents to require the data's disclosure. Preservation has been the law in the U.S. since April 1996.[93]

In Canada, ISPs have raised concerns about the cost of data retention, as they have with other aspects of Internet enforcement. While it is beyond the scope of this report to address the issue, the Supreme Court of Canada recently confirmed that police do not have to pay for third parties (in this case, a phone company) to produce records needed in criminal investigations.[94] The Court heard evidence that the annual cost of TELUS to comply with production order requests would be over $660,000, which represents 0.023 percent of operating revenue for 2004 and 0.058 percent of Telus' earnings—"...the equivalent of a person earning $100,000 a year having to spend up to $58 to comply with jury duty."[95]

Benjamin Perry, assistant law professor at the University of British Columbia, contends, "Internet service providers do make a lot of money off of the sharing of child pornography online" and they "have an obligation to contribute more to eradicate child pornography than they do now."[96]

RECOMMENDATION 3—That the federal government introduce legislation to require ISPs to retain customer name and address data, traffic data and content data for two to five years.

4. ACCESSING AND STORING INFORMATION

Even when authorities are able to obtain customer name and address information, they may still hit roadblocks if they come across offenders who have password-protected or heavily encrypted computer systems.

While authorities obviously make every effort to get the offender to cooperate, there is no provision in current legislation that makes it a crime for offenders to withhold this information. Evidently, offenders are not inclined to give this information willingly, as they know it may lead to evidence and material that could be used against them in a court of law.

Some law enforcement organizations report cases where they have not been able to access a computer because they could not break the encryption. In these cases, there is no other option than to drop the charges. As the technology becomes more sophisticated and online predators become increasingly savvy, police are concerned that more and more people will encrypt their computers.

There are certain provisions in the *Criminal Code of Canada* that address cooperation as required when police suspect someone of driving while under the influence of alcohol. For example, it is a criminal offence to refuse to take a breathalyzer test when police suspect a person of impaired driving. In the same way that police are unable to assess the level of the driver's inebriation, law enforcement cannot evaluate the scope of the problem with child sexual abuse images until they are able to access the location where they are contained.

[93] 18 U.S.C. 2703(f) requires an electronic communications service provider to "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process" upon "the request of a governmental entity."

[94] *Tele-Mobile Co. v. Ontario*, 2008, SCC 12.

[95] Ibid., p. 36.

[96] Canwest News Service, "Internet service providers profit from online child porn, legal expert says," *National Post*, December 1, 2007.

Similarly, provisions could be included to make it a criminal offence not to provide a password to law enforcement in cases of suspected possession of child sexual abuse images. Although the charge of not providing a password could be lesser than the charge and sentence for possessing and/or distributing the images, the offender would still have a criminal record, may be required to register with the National Sex Offender Registry, may be required to submit DNA to the National DNA Database and would have to forfeit his or her computer.

Subsection 153.1(*b*) of the *Customs Act* makes it an offence to hinder or prevent an officer from conducting his or her duties as authorized by the Act, including searches. This section has been used with respect to individuals who did not want to provide passwords for portable computers. In addition, laptops can be detained (section 101) until they are examined.

The U.K. and Australia already have in place legislation to assist law enforcement to access computers and equipment that are protected by passwords or encryption. In the U.K., legislation allows law enforcement authorities to ask anyone who has protected electronic data (e.g. encrypted) or who has access to the data's encryption keys to either give the police the data in a readable format, or to give them the encryption key so it can be accessed.[97] Failure to do so can result in a jail sentence of up to two years (five years if the matter is one of national security). It is also a criminal offence if disclosure is not made in compliance with an order.

In Australia, police can apply to a magistrate for an order requiring a person to provide any information or assistance that is reasonable and necessary to allow the officer to access data held in a computer. A person who fails to comply with the order is liable to six months' imprisonment.[98]

Canada needs to give authorities the ability to access the evidence. If the courts give law enforcement the right to search a computer, we believe it must also provide the power for police to act on this right and to hold the individual accountable.

RECOMMENDATION 4—That the federal government introduce legislation to amend the *Criminal Code* to make the refusal to provide a password or encryption code upon judicial order a criminal offence.

[97] Part III of the *Regulation of Investigatory Powers Act 2000*.

[98] CRIMES ACT 1914 - SECT 3LA. Person with knowledge of a computer or a computer system to assist access, etc. www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s3la.html.

5. IDENTIFYING VICTIMS THROUGH IMAGE ANALYSIS

Traditionally, police have focused on catching offenders, but with the increase in the creation and distribution of child sexual abuse images and the use of new technologies such as the Internet, police services have new tools they can use to find victims, and are starting to focus more resources in this area. This is especially helpful in the area of child sexual abuse, where many victims do not report crimes to police.

The identification of victims is achieved by image analysis—a highly specialized, exacting and time-consuming process that is conducted by individual law enforcement officers who must devote countless hours to deciphering the clues in the pictures. It is, in effect, good "old fashioned" police work, but done with high-tech tools in a digital environment.

Image analysis has resulted in the rescue of hundreds of children worldwide. In 2003, Toronto police began investigating a series of hundreds of images of the same child. Through a tiny wrist band she had on and a one-millimetre blurred photograph of a logo on a uniform, they traced the child to North Carolina. Authorities there identified her and arrested her father, who is now serving a sentence of 100 years.[99]

The same year, Winnipeg police reviewed a 14-minute video that involved the abuse of two young girls and noticed several clues. They heard a radio station's call letters, saw tattoos on the abuser and noticed a 1996 U.S. election poster. Winnipeg police notified the U.S. Customs Service International Child Pornography Investigation and Coordination Center, which traced the radio station to Connecticut. Customs had an older video of one of the girls (which meant she had suffered abuse for years) and age-enhanced the photos, which led to the girls' identification and rescue.[100]

More recently, in 2008, Toronto police arrested a former children's store employee after discovering 30,000 computer child sexual abuse images on his computer. Police were able to identify three of the victims, whose parents were not aware of the alleged abuse before police intervened.[101]

Image databases

To help coordinate efforts to identify children through image analysis and manage huge volumes of evidence, law enforcement agencies around the world are developing databases of known child sexual abuse images.

INTERPOL, the world's largest international police organization, created a database called the INTERPOL Child Abuse Image Database (ICAID). ICAID has been endorsed by the G8 and has hundreds of thousands of images which are submitted by member countries, including Canada. The ICAID uses image recognition software to compare details of where the abuse took place, to connect images from the same series of abuse, or to identify images taken in the same location with different victims. Once a country of origin can be established, the images are sent to police in the countries concerned for follow-up. Investigators have been able to identify and rescue several hundred victims using this system.[102]

[99] Associated Press, "Child pornographer jailed for 100 years," *Montreal Gazette*. October 21, 2006.
[100] Jason van Rassel, "Manitoba police making headway," *Calgary Herald*. June 13, 2006.
[101] Michele Henry, "Police find Toronto child porn victims—Man, 36, charged after 30,000 images seized," *Toronto Star*, October 17, 2008.
[102] INTERPOL Fact Sheet on Crimes Against Children. www.INTERPOL.int.

By sharing images, law enforcement across the country and around the world have a chance to speed up rescue efforts. In one case, images found in Germany were placed in an international INTERPOL database. A Canadian law enforcement officer noticed a cap from a school in New Brunswick, which eventually led to the identification of victims. Without the database, this identification may never have occurred or it might have taken months.

Another way these databases help is by providing information on those victims who have already been identified and rescued, even if their images continue to circulate and be shared. Marking these images with this information could save other law enforcement agencies countless hours and resources, which are better spent on looking for children who are still being abused.

The U.S. has incorporated the building of these databases directly into its investigative process. Law enforcement agencies are required to send all images to the National Center for Missing and Exploited Children (NCMEC). NCMEC's Child Victim Identification Program, created in 2003, serves as the national clearinghouse for child pornography cases across the country and is the main point of contact for international agencies.[103] Its analysts work to identify victims and individuals who sell, trade and distribute the images. To date, NCMEC has processed at least 15 million images and videos and has helped identify over 1,600 children. In one case, a series of images involving one young girl was tracked to over 13,000 individual investigations in the U.S. alone.

In the U.K., the Child Exploitation and Online Protection Centre (CEOP) has also created an image database, which has directly contributed to the rescue of more than 18 children.[104]

Canada is also making strides to create a similar database. The RCMP's National Child Exploitation Coordination Centre (NCECC) is the clearinghouse and coordination centre for international requests to conduct investigations in Canada related to child sexual exploitation on the Internet. NCECC is working to have a database operational shortly. Ultimately, the success of the database will depend on law enforcement agencies forwarding all images to the NCECC.[105]

Building expertise

Since image databases cannot automatically identify the children in the images, it is important that both the time-consuming and specialized work of image analysis as well as the development of databases and information-sharing tools be well supported.

The Ontario coordinated provincial strategy, led by the Ontario Provincial Police, includes victim identification/background analysis teams that analyze child abuse images for clues of the children's whereabouts. The integrated model coordinates the increased identification, provides support services to child victims (and their families) of Internet sexual abuse and exploitation, and assists in preventing the cycle of recurring victimization.[106]

The expansion and strengthening of "corporate knowledge" in the area of victim identification is crucial and fundamental to a meaningful response to victims of sexual abuse; without it, the children simply go on in their suffering. The NCECC has, as part of its mandate, the responsibility to identify victimized children. The Centre can provide a number of services to law enforcement, including expertise in victim identification techniques. This expertise must be supported and built upon.

103 NCMEC's Child Victim Identification Program does not retain actual photos of the children. www.cybertipline.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=2444.

104 www.ceop.gov.uk/mediacentre/statistics.asp.

105 Two provinces, Ontario and Quebec, have legislative requirements mandating law enforcement agencies submit reports to the Violent Crime Linkage Analysis System (ViCLAS), an automated national database case linkage system designed to capture, collate and compare crimes of violence through the analysis of victimology, offender/suspect description, modus operandi, forensic and behavioural data. ViCLAS is operated by the RCMP and its success is dependent upon the number of officers who submit reports to it. There are over 300,000 cases on the system and over 3,000 linkages have been made, but participation is not universal.

106 Ontario's Provincial Strategy to Protect Children from Sexual Exploitation and Abuse on the Internet, PowerPoint presentation, January 2008.

Responsible image management

While image databases have obviously proven useful, there is an obligation to remain conscious of the impact that the storage and sharing of these documents may have on the victims. The international organization End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes warns, "Knowledge of the existence of images in police databases may be just as harmful to the child."[107] For victims, it may not matter who is looking at their photos or why they are being used. They have no control over who has access to them, if they are ever removed, etc.

The NCECC is aware of the privacy implications for victims of having their photos included in law enforcement databases and is preparing a Privacy Impact Assessment for the Federal Privacy Commissioner. The Centre will continue to dialogue with the Office of the Federal Ombudsman for Victims of Crime as policies are developed.

RECOMMENDATION 5—*That the federal government, in partnership with the provinces, develop a national strategy to identify victims found in child sexual abuse images and that the strategy includes an expansion of the National Child Exploitation Coordination Centre's National Victim Identification Unit and support for the national image database.*

[107] "Violence Against Children in Cyberspace," ECPAT International, 2004.

6. HELPING VICTIMS HEAL

"A nine year old girl was abused by her uncle and the only reason she agreed to come to the centre was because her mom told her she would only have to tell her story once. That was one Friday afternoon. On Monday afternoon, after school, she cleaned out her piggy bank and asked her mom to take her to Toys R Us. She had enough money to buy three stuffed animals. She dropped them off at the front counter here and said, 'These are for the next three kids who come to Zebra.'"[108]

–Barb Spencer, Executive Director, Zebra Child Protection Centre

"Not having such a centre available in other major cities defies belief; it is like the subtle difference between holding a hand and chaining a soul for the children who need this protection...."

–Mother whose son was sexually abused and who attended the Zebra Centre

Child advocacy centres: A model for success

First developed in the U.S. in the 1980s, Child Advocacy Centres (CACs) were designed to reduce the stress on child abuse victims and families created by traditional child abuse investigation and prosecution procedures and to improve the effectiveness of the response.[109]

A victimized child and his or her family can go to more than 10 different locations and see multiple professionals before getting help.[110]

These professionals are often working in isolation and do not communicate efficiently or effectively with the child and family, or with each other. The result is a fragmented, confusing, inefficient and expensive process. CACs, on the other hand, provide an integrated approach to helping children who have been victims of abuse by bringing together key victim services, such as statement collection and counselling, in one child- and family-friendly location.

The National Network of Children's Advocacy Centers, now called the National Children's Alliance (NCA), was formed in 1988. It is a U.S. nationwide not-for-profit membership organization whose mission is to promote and support communities in providing a coordinated investigation and comprehensive response to victims of severe child abuse. There are over 900 CACs and over 600 are certified with the NCA.[111]

108 Jamie Hall, "Shedding light on the darkest of crime," *Edmonton Journal*, September 29, 2007.

109 Theodore P. Cross et al., "Evaluating Children's Advocacy Centres' Response to Child Sexual Abuse," Office of Juvenile Justice and Delinquency Programs, August 2008. www.ncjrs.gov/pdffiles1/ojidp/218530.pdf.

110 BOOST Child Abuse Prevention & Intervention.

111 Under the U.S. federal *Victims of Child Abuse Act*, the NCA receives funds from the American Department of Justice, Office of Juvenile Justice and Delinquency Prevention, and distributes funds to local communities to support the growth, continuation and development of CAC programs nationally. Certified CACs may receive annual funding.

Although the services offered vary, there are some key elements necessary to gain accreditation from the NCA:

1. *Child-appropriate/child-friendly facility:* The CAC provides a comfortable, private, child-friendly setting that is both physically and psychologically safe for clients.
2. *Multidisciplinary team:* This multidisciplinary team for response to child abuse allegations includes representation from law enforcement, child protective services, prosecution, mental health, medicine and victim advocacy.
3. *Cultural competency and diversity:* The CAC promotes policies, practices and procedures that are culturally competent; cultural competency being defined as the capacity to function in more than one culture, requiring the ability to appreciate, understand and interact with members of diverse populations in the local community.
4. *Forensic interviews:* Forensic interviews are conducted in a neutral, fact-finding manner and are coordinated to avoid duplicative interviewing.
5. *Medical evaluation:* Specialized medical evaluation and treatment are to be made available to CAC clients as part of the team response, either at the CAC or through coordination and referral with other specialized medical providers.
6. *Therapeutic intervention:* Specialized mental health services are to be made available as part of the team response, either at the CAC or through coordination and referral with other appropriate treatment providers.
7. *Victim support/advocacy:* Victim support and advocacy are to be made available as part of the team response, either at the CAC or through coordination with other providers, throughout the investigation and subsequent legal proceedings.
8. *Case review:* Team discussion and information sharing on the investigation, case status and services needed by the child and family are to occur on a regular basis.
9. *Case tracking:* CACs must develop and implement a system for monitoring case progress and tracking case outcomes for team components.

Research suggests that these centres are having a real impact that is measurable not just in terms of its benefits to victims and their families, but in dollars.

The National Children Alliance Annual Report states that an investigation into a child abuse case in a community with a CAC is 45 percent less expensive than in a community without a CAC.[112]

Similarly, evaluations from the Crimes Against Children Research Center found jurisdictions with CACs allow for more coordinated investigations, higher rates of referrals for mental health services and suggest parents are more satisfied and children are less scared.[113]

The United Nations Resolution on Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime, which Canada spearheaded, reflects many of the same principles that guide CACs. For example, the resolution recognizes that children are particularly vulnerable and "need special protection, assistance and support appropriate to their age, level of maturity and unique needs in order to prevent further hardship and trauma that may result from their participation in the criminal justice process."[114]

[112] *National Children Alliance Annual Report 2005*. www.nca-online.org/uploads/NCA%20AR2005.pdf.
[113] Crimes Against Children Research Center, "Executive Summary: Findings from the UNH Multi-Site Evaluation of Children's Advocacy Centers." www.unh.edu/ccrc/.
[114] www.un.org/docs/ecosoc/documents/2005/resolutions/Resolution%202005-20.pdf.

The guidelines stress that:

- To avoid further hardship to the child, interviews, examinations and other forms of investigation should be conducted by trained professionals who proceed in a sensitive, respectful and thorough manner. Special services and protection will need to be instituted to take account of gender and the different nature of specific offences against children.
- Professionals should make every effort to coordinate support so that the child is not subjected to excessive interventions. The child should receive assistance from support persons, such as child victim/witness specialists, commencing at the initial report and continuing until such services are no longer required.

Child advocacy centres in Canada

In a report prepared for the Law Commission of Canada, researchers estimated the cost of child abuse for Canadian society in 1998—including judicial, social services, education, health, employment and personal costs—was $15,705,910,047.[115] They also found that in general, the major costs of child abuse are not borne by the Government, but instead are personal costs to the victims. "Our research strongly suggests that it is false economy to save dollars in the short run by ignoring abuse or by cutting programs designed to help families. There is a tremendous imbalance in what we as a society allocate to reduce the effects of abuse and the costs themselves."[116]

"Even a relatively small increased investment in effective prevention and treatment programs could yield huge dividends for society. In fact, the earlier the intervention, the lower the overall costs and the greatest chance there is for a reduction of the multiplier effects consequent to abuse."[117]

In Canada, only a few programs offer services similar to those of the CAC model. The Edmonton Zebra Centre (2002) is the only program currently affiliated with the NCA. Other examples of similar programs include the newly created Niagara Child Advocacy Centre (2008)—which hopes to receive accreditation from the NCA—the Regina Children's Justice Centre (1994), the Gatehouse and the BOOST Centre in Toronto. Several other communities are exploring CACs for their jurisdictions but in some cases funding has been identified as a barrier.

The benefits of CACs in the U.S. are also being seen in Canada. The Edmonton Zebra Centre has specially trained forensic interviewers who conduct the interviews with children. Police and child welfare officers observe the interviews but do not question the child. The centre has proven that the CAC model and coordinated investigations get proven results. Specifically, it has found that the CAC model leads to a reduction in system-induced trauma for victims, an increase in charges laid, better quality of evidence, more guilty pleas and higher convictions rates with more appropriate sentences.[118] On top of that, the Zebra Centre has also found that families are generally more willing to access services if they are on-site.

Conversely, the BOOST centre warns that, "...a lack of coordination and organization negatively affects victims who do not receive the maximum amount of benefit from services and the legal system."[119]

[115] Audra Bowlus, Katherine McKenna and David Wright, *The Economic Costs and Consequences of Child Abuse in Canada*, Law Commission of Canada, 2003, p. V. http://dsp-psd.pwgsc.gc.ca/collection_2007/lcc-cdc/JL2-39-2003E.pdf

[116] Ibid., p. 91.

[117] Ibid., p. 92.

[118] *ZEBRA Child Protection Centre, Victims of Crime Fund Grants Program Evaluation Report*, March 1, 2007, p. 9.

[119] BOOST Child Abuse Prevention & Intervention. "Responding to Child & Youth Victims of Sexual Exploitation on the Internet: Best Practice Guidelines." www.boostforkids.org., p. 15.

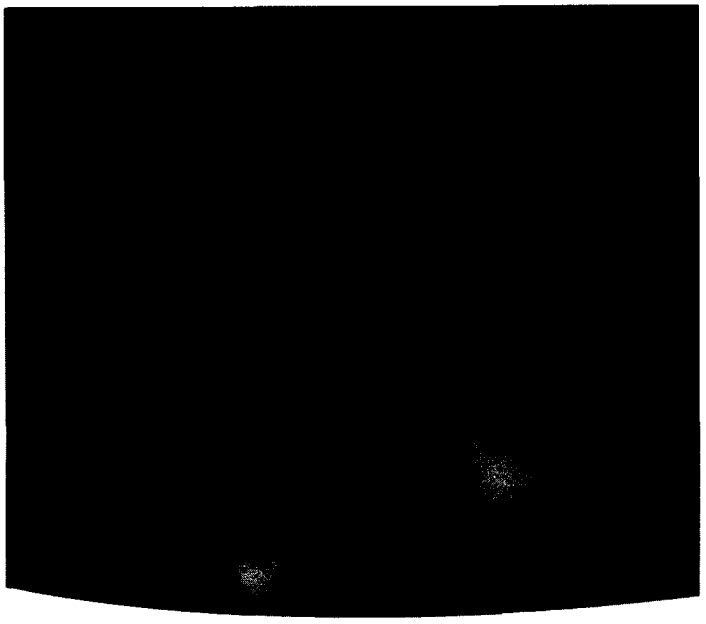
How child advocacy centres can help victims of Internet-facilitated child sexual abuse

Given the unique dynamics surrounding child sexual abuse images and the benefits of a coordinated approach, CAC models could be particularly relevant in investigations involving child sexual abuse images. They could help to obtain more information from children (i.e. existence of photos), recognize the signs of when a child may not be disclosing, and provide guidance on how to handle a situation where images have been found but the child is not disclosing or not aware, and more.

According to BOOST, interviewing victims of child sexual abuse imagery crimes may require a different strategy, compared to conventional sexual abuse:

"Due to the fact that abuse imagery on the Internet is a permanent record of maltreatment, children in these situations often do not disclose full details of the abuse until they have recovered from the initial trauma of realizing that others will see the pictures in the future. In addition, child abuse imagery is physical evidence of a crime scene, and thus, investigators aim to acquire knowledge about the offender(s) and not the crime itself. Consequently, when investigators (and treatment providers) speak with children, interviews should span over a period of weeks to months. Questions should be general in nature, focus on the offender(s)' identity, and the possibility of other children currently being victimized; they should not discuss details of the abuse; and, they should not focus on the nature of the abuse, as those working with the children will already know what has happened, and discussing the abuse will be psychologically harmful for the child."[120]

Some of this work is already underway. The Northern Alberta Integrated Child Exploitation (ICE) Team actively works with the Zebra Centre to help victims of child sexual abuse.



[120] Ibid.

It is clear from the evidence that CACs are a proven, results-oriented and victim-friendly way to ensure better victim care, higher conviction rates and lower systemic costs.

For that reason, the Federal Ombudsman for Victims of Crime wrote to the Minister of Finance in advance of Budget 2009 to request that $5 million be allocated toward the support of these centres across the country. While the recommendation was not included in the January budget, there is still an opportunity for the federal government to take action.

RECOMMENDATION 6—That the federal government, in conjunction with provincial and municipal governments, develop a national strategy to expand the network of Child Advocacy Centre models in communities across the country.[121]

7. LEARNING TO BETTER HELP VICTIMS

"Long term effects of being photographed were more debilitating...exacerbated by the knowledge that others may see or distribute the films...knowledge that photos may be used to exploit other children."[122]

"Little is known about the full and long term impact of being used in pornography upon children and their families, their coping strategies and the support they do or do not receive."[123]

Therapists, law enforcement and victim services have years of experience dealing with child sexual abuse victims, but there is growing recognition that the making of child sexual abuse images and their distribution complicate the aftermath of the sexual abuse. This has an impact on the recovery of victims and the delivery of services to those victims.

"Due to its relatively new nature, the Internet adds novel and specific elements of victimization that have never been present in the past. Of particular concern is the fact that the Internet provides a permanent, uncontrollable record of abuse; if child sexual abuse images of videos of victimization exist on the Internet, they will never disappear. This aspect of victimization has devastating effects on victims including: victim silencing; self-blame for the abuse; increased levels of trauma; shame and embarrassment knowing that others have/will see the abuse on the Internet; decreased amounts of disclosure; and, victims taking a longer amount of time to recover from the abuse in comparison to exploitation without recording."[124]

Given these complications, it is necessary that the professionals who are helping victims and their families learn more about dealing with this particular type of abuse, methods for coping and signs of further distress.

121 It is important to emphasize the importance of community involvement in developing a CAC and that no one model will work for every community.

122 M.H. Silbert, Effects on Juveniles of Being Used for Pornography and Prostitution, in D. Zilman and J. Bryant (eds.), *Pornography: Research Advances and Policy Considerations*, Lawrence Erlbaum Associates, 1989.

123 Susan J. Creighton, "Child pornography: images of the abuse of children," November 2003, www.nspcc.org.uk.

124 BOOST Child Abuse Prevention & Intervention, "Responding to Child & Youth Victims of Sexual Exploitation on the Internet: Best Practice Guidelines," www.boostforkids.org., p. 1.

Dr. Sharon Cooper recommends that those who work with child sexual abuse victims,

"...have to learn how to ask the right questions about the possibility that a child's victimization may have entailed production, dissemination, possession or extortion through the use of child sexual abuse images..." because "...children not only typically do not tell of their abuse, but will in fact deny the presence of images.... This background of having pictures and videos taken of one's sexual abuse is a significant risk factor for substance abuse, mental health problems and run away behaviours."[125]

Recently, the Supreme Court of Canada recognized the additional suffering that the distribution of child sexual abuse can cause when it reinstated a more severe sentence for a father who was convicted of sexually assaulting his 4-year-old daughter and of making, distributing and possessing child pornography. At the time of his arrest, his computer contained approximately 5,300 pornographic photographs and 540 pornographic videos involving children, many of which included his daughter. The trial judge imposed the maximum sentence of 10 years for sexual assault and another 5 years for the other offences but the Court of Appeal reduced the sentence from 15 to 9 years. Supreme Court Justice LeBel said, "I note that L.M. disseminated his pornography around the world over the Internet. The use of this medium can have serious consequences for a victim. Once a photograph has been posted on the Web, it can be accessed indefinitely, from anywhere in the world. R.M. will never know whether a pornographic photograph or video in which she appears might not resurface someday."[126]

At the victims' level, a psychological assessment and treatment model is being developed for children and their families as part of the Ontario Provincial Strategy to Protect Children from Sexual Abuse and Exploitation on the Internet.[127] Additionally, the Ontario Victim Services Secretariat at the Ministry of the Attorney General offers a program to pay for counselling for young victims of sexual exploitation on the Internet who were under the age of 18 when the crime took place. The program also helps their family members. Over 385 victims have been assisted in Ontario and over 90 people have accessed the special compensation fund to assist victims and their families to access counselling.[128]

Answering tough questions

The problem is that there has been little research into these issues. According to BOOST, "Among many regions, there is a lack of understanding about the experience of victims who have been sexually exploited on the Internet... compared to other forms of child maltreatment, there is a relatively small amount of research and literature about Internet child exploitation."[129]

125 Dr. Sharon Cooper, Oral Testimony for the United States Senate Committee on Commerce, Science and Transportation, September 19, 2006.

126 *R. v. L.M.*, 2008 SCC 31, para. 28. This case resulted from an investigation by Switzerland police into groups distributing child sexual abuse images on the Internet. Switzerland police alerted Quebec authorities about the two Quebeckers who had been identified in Internet user groups. Had this investigation into the distribution of child sexual abuse images not taken place, a father would still be abusing his daughter today.

127 Dr. Jennifer Coolbear and Tanya Smith, Toronto Hospital for Sick Kids, BOOST—Responding to Child and Youth Victims of Sexual Exploitation on the Internet Conference, Collingwood, Ontario, September 2007. Part of the strategy includes coordinating the identification of victims and providing support services, and Ontario has developed a special compensation program for victims and has provided compensation to over 300 victims.

128 Direct victims may receive up to $1,500 for counselling and family members may receive up to $800.

129 BOOST Child Abuse Prevention & Intervention, "Responding to Child & Youth Victims of Sexual Exploitation on the Internet: Best Practice Guidelines." www.boostforkids.org., p. 11.

Despite the successes, the relatively small number of victims who have been identified and their young age, combined with the lack of experience with the long-term impacts that these images may present, means there are many questions but few satisfactory answers at this time. So far, much of the work victim services have done is with adolescent females who have been targeted by adult men online, and these cases may present entirely different dynamics than cases involving images and abuse.[130]

More work needs to be done to answer some important questions. What should be done when victims have grown up but are unaware that images were made? What should happen when law enforcement discovers old images? Should those victims be notified (if they are identified)? If so, how? At what age? What if a child does not disclose that images were made? If a child denies the images or videos, should the child be challenged?

As Jonah Rimer stated, "Very little is known about the psychological effects on adults who are told that there are child abuse images of them on the internet and careful thought must go into the time and way in which such a revelation should take place."[131]

There are also the questions that surround victims who know already that these images exist. Victims may be concerned about how those viewing the images (i.e. police officers) may perceive them. Many abusers force victims to appear as if they are enjoying what is happening, and therefore a victim may be concerned that police will think they really enjoyed it. Child sexual abuse images and videos may, in some cases, challenge the perceptions and beliefs that authorities have of child sexual abuse victims (i.e. that they are always non-compliant victims forced to perform).

Retired FBI Agent Kenneth Lanning said, "Society has a problem dealing with any sexual-victimization case in which...the child victim is not completely good. The idea that child victims could simply behave like human beings and respond to the attention and affection of offenders by voluntarily and repeatedly returning to an offender's home is a troubling one. It confuses us to see the victims in child pornography cases giggling or laughing."[132]

The international organization End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes also makes the point that "Practitioners report that a child in this situation may feel that the existence of imagery of their humiliation masks the violence they have experienced and makes them appear complicit. This dilemma adds an extra traumatic burden."[133]

Sexual abuse is never the child's fault as they are legally incapable of consent. But for some victims, the abuse has become so normalized that they have adopted coping methods that may shock us. One investigator described one case where he saw the grooming of a victim, which started with taking normal photos, then led to harmless play, culminating in sexual abuse. At the "end" of the process, the victim was directing some of the abuse, negotiating for presents or money to participate and perform certain acts.

For these reasons and more, victims often do not disclose that photos were taken or videos were made. Even when confronted with such discoveries, some victims will

[130] For example, some of these teens may not identify themselves as victims. In a high-profile case involving a Kingston man who manipulated hundreds of girls worldwide into performing sexual acts in front of a webcam and threatened them with exposure of the images, law enforcement reports that some of the girls did not think it was that serious. It remains to be seen what the long-term impacts of such victimization may be.

[131] Jonah Rimer, *Literature Review—Responding to Child & Youth Victims of Sexual Exploitation on the Internet*, 2007, p. 52.

[132] Kenneth V. Lanning, "Overview of Sexual Victimization of Children," adapted from the National Center for Missing and Exploited Children, *Child Molesters: A Behavioural Analysis* (4th ed.), 2001.

[133] ECPAT International, "Violence Against Children in Cyberspace," 2005, p. 41.

refuse to acknowledge their existence. Children "can easily suffer further harm if they are pressured to verify the authenticity of an abuse image."[134]

This must be taken into consideration when law enforcement makes a decision on how to approach child victims to learn more information about the offender or the crime.

Law enforcement techniques that may be helpful in traditional child sexual abuse cases need to be re-examined in cases involving child sexual abuse images. For example, police often videotape children giving statements in cases of child sexual abuse. In Canada, these videos may be used in court and can be beneficial to the prosecution of child sexual abuse cases. But concerns have been raised that "...taking video evidence from a child already forced to make abuse images could further the harm done to the child."[135] For children who have been the subject of abusive images, the use of a televized link may trigger memories or flashbacks to their abusive experiences.

All in all, it is clear that a lot of work needs to be done to help law enforcement, psychologists, counsellors and other key professionals understand how best to help victims of Internet-facilitated child sexual abuse.

RECOMMENDATION 7—That the Department of Justice's Policy Centre for Victim Issues fund research into the needs of victims of Internet-facilitated child sexual abuse.

8. ENDING ONGOING VICTIMIZATION

"This is how I see it. When I capture their image—I capture a piece of time that not even there own mommy's will have. They stay young forever, just for us pedos.... The vid cam makes them our eternal slaves. They becum our property to do whatever we want too."

–Written in a chat message by Darren Philpott/canuckboylover[136]

"Usually, when a kid is hurt and the abuser goes to prison, the abuse is over. But because XXX put my pictures on the Internet, the abuse is still going on.... I am more upset about the pictures on the Internet than I am about what XXX did to me physically."

–13-year-old sexual abuse victim whose images were put on the Internet

As determined, the ongoing circulation of child sexual abuse images makes it exponentially more difficult for victims to move on and heal.

While the abuse itself may have taken place in the past, victims are continually traumatized by the fact that those images continue to circulate and be used for gratification purposes. This is compounded by the fear that such personal markers of their own private past could pop up anywhere, for anyone to see at any given time.

[134] Ibid., p. 42.
[135] Ibid., p. 42.
[136] Jana G. Pruden, "He's dead, but the abuse lives on...," *Leader-Post*, November 22, 2008. Philpott was awaiting trial on child pornography and child sexual abuse when he committed suicide.

Such ongoing levels of anxiety would be difficult for anyone to bear. For a victim who not only feels the embarrassment and shame of the image itself, but is forced to relive the crime each time the image is viewed, it is excruciating.

Consequently, it is imperative that any consideration of this issue include a discussion and recommendation on the handling of child sexual abuse images once they have been identified.

The handling of images falls into two main spheres—the lawyers and law enforcement specialists who handle and store the images as evidence and the Internet itself where the images are circulating.

Handling of child sexual abuse images in the Canadian justice system

In Canada, Crown attorneys are obligated to disclose copies of all evidence to the defence, including child sexual abuse images. These images are, however, unique and, given the serious privacy implications that exist for such victims, special care must be taken with respect to their disclosure.

This has already been recognized in the U.S. where legislation provides that in child pornography prosecutions, any property or material that constitutes child pornography shall remain in the care, custody and control of either the Government or the Court and that courts shall deny any request by the defendant to copy, photograph, duplicate or otherwise reproduce any property or material that constitutes child pornography so long as the Government makes the property or material reasonably available to the defendant.[137]

In 1993, the Ontario Attorney General's Advisory Committee on Charge Screening, Disclosure and Resolution Discussions ("the Martin Committee") recognized that while the "normal method" of disclosure was by copy, other interests, including

[137] Title 18, section 3509 of the U.S. Code.

a reasonable privacy or security interest of a victim or witness, may require and allow for an alternative form of disclosure, such as private viewing.[138]

In *R. v. Blencowe*, which involved the disclosure of 35 videotapes alleged to contain child pornography, Mr. Justice Watt found that while disclosure to defence counsel was mandatory, it was also necessary to consider the privacy interests of the victims and that they not be further compromised by copying, viewing, circulation or distribution of the tapes beyond what was required. Justice Watt required defence counsel to sign an undertaking with certain conditions prior to receiving disclosure. He proposed several conditions, including that counsel retain possession and control of the copies and not release them to anyone other than an expert; that the defendant not have possession or control of the tape (or images); that no one be permitted to view the tapes (or images) except the applicant, his counsel and any expert; that no copies be made and that the tape (or images) be returned to the investigating officer.[139]

More recently, in October 2008, an Alberta Provincial Court judge imposed strict conditions for the defence lawyer to abide by upon receipt of the DVD from the Crown: A lengthy password, which could not be written down, was given to him so he could access the evidence on the encrypted DVD; he could not allow anyone else to view the evidence; the DVD had to be returned to the Crown for destruction; and finally, he had to turn over the computer used for viewing the evidence to have an expert delete everything.[140]

In Canada, defence attorneys may be required to enter into an undertaking or to apply for a court order under subsection 490(15) of the *Criminal Code* to obtain access to the seized images, pursuant to conditions similar to those set out above (although more stringent).[141] Unfortunately, an undertaking is no guarantee that a child's privacy will not be compromised. On at least two occasions, defence counsel in Ontario have lost or misplaced material and were not able to return it to the police.

Finally, once the evidence has been viewed and removed it should be deleted from the original computer system in accordance with the *Criminal Code*. Subsection 164.1(5) of the *Criminal Code* allows the Court to make an order to the "custodian of the computer system" to delete material that the Court is satisfied, on a balance of probabilities, is child pornography.[142] There is little evidence, however, to show that courts are making these orders. We therefore urge the Department of Justice to consult with its provincial and territorial counterparts to determine if these provisions are being used as Parliament intended and if they need to be amended to provide more clarification for the Court.

RECOMMENDATION 8—That the federal government introduce legislation to amend the *Criminal Code* to ensure that child sexual abuse images, video or audio recordings are not disclosed to defence counsel but that opportunities are made available for proper review of the evidence.

138 *Report of the Attorney General's Advisory Committee on Charge Screening, Disclosure and Resolution Discussions*, 1993, pp. 235–236.

139 *R. v. Blencowe* (1997) O.J. No. 3619.

140 "Lawyer can view alleged child porn," *Calgary Herald*, October 24, 2008.

141 Subsection 490(15) of the *Criminal Code* provides for a court to make an order allowing a person who has an interest in items seized by the police to examine anything so detained. Subsection 490(16) provides for the court to place conditions on the order allowing access in order to safeguard and preserve the items in question. Section 605 provides a mechanism for the courts to balance competing interests and impose conditions when contraband is released to defence counsel (i.e. guns or drugs released for scientific testing) pursuant to section 605 of the *Criminal Code*.

142 According to a 2001 Department of Justice backgrounder, Bill C-2 suggests "custodian of a computer system" includes ISPs.

9. STEMMING THE FLOW OF CHILD SEXUAL ABUSE IMAGES OVER THE INTERNET

"The simplicity of getting material...it's close to mind-boggling. I have never understood how come the whole thing wasn't shut down. You search for the word 'baby' and it will find stuff there...it's easy...."

-Michael Briere, murderer of Holly Jones[143]

"I never escape the fact that pictures of my abuse are out there forever. Everything possible should be done to stop people looking at pictures of child abuse. Each time someone looks at pictures of me, it's like abusing me again.[144]"

-16-year-old girl named Sandra

"Growing up and trying to fit into a normal life after so much abuse is hard. I have nightmares, flashbacks and struggle with everyday tasks that most people take for granted.... There is a haunting that surrounds me constantly, reminding me that I don't have control over keeping my past a secret. The pictures that were taken when I was so young are still out there. Who knows where they are and how many people have seen them. I wonder if they will show up when I least expect it. I am away from abuse now, but know that someone could be pleasuring himself while looking at my pictures or showing them to kids."

-A victim[145]

There is unfortunately no magic button or software that can locate and destroy all child sexual abuse images on the Internet. Once an image is released, it is impossible to get back. The image becomes part of an endless cycle of abuse as it is shared by countless predators and may be used to groom other victims.

That being said, there are measures that can be taken by both government and the private sector to help curb the spread of the material and deter abusers from accessing it.

At the 2007 G8 Justice and Home Affairs Ministers meeting, all Ministers recognized that the war against Internet predators could not be won by law enforcement alone.[146] They acknowledged that the private sector has an important role in protecting the world's children.

Working with the private sector

There are some positive examples of industry leaders accepting responsibility for their role in preventing the spread of child sexual abuse images. For example, AOL—an online service provider—developed the Image Database and Filtering Process, which allows AOL to proactively and automatically locate known child sexual abuse images moving through its system, delete them and route a report to law enforcement.[147] In one of its first cases, AOL notified the NCMEC that an AOL user had tried to upload a single image to his email account. Within a week, the local police had a search warrant and arrested a California man. His arrest led to the identification of 35 other people involved in trading images. On top of it, the California man, who was a youth baseball coach, admitted he had abused a child.

MSN uses a filtering tool to review images uploaded to MSN Spaces and MSN Groups. Images that are flagged as potential child sexual abuse images are reviewed and,

143 Canadian Press, "Michael Briere says he was spurred by kiddie porn in sex slaying of Holly Jones," *Peterborough Examiner*, June 18, 2004.
144 Internet Watch Foundation.
145 Monique Mattei Ferraro and Eoghan Casey, "Investigating Child Exploitation and Pornography," Elsevier Academic Press, 2005, p. 3.
146 G8 Justice and Home Affairs Ministers, May 24, 2007, www.g8.gc.ca/childpornography-en.asp.
147 Julian Sher, *Caught in the Web*, Perseus Publishing, 2007, p. 232.

if deemed appropriate, a report is sent to the NCMEC.[148] MSN closes the site and preserves the entire site, account information and associated files.

This software used by MSN and AOL focuses on images that are a part of the NCMEC database. The technology is not a cure-all as it does not apply to new images, but it is an important first step. If all ISPs participated, it could have an impact on the child sexual abuse image industry as a whole by helping to prevent the dissemination of child sexual abuse images, thereby preventing further exploitation of some victims.

The same type of technology could be developed in Canada to identify and remove images that are found within the Canadian NCECC child sexual abuse imagery database. By blocking the dissemination of these photos, Canada could have a real impact on stemming the flow of these abusive images.

Project Cleanfeed is another example of a successful private initiative. The U.K.-based filter helps participants, such as British Telecom, to block approximately 35,000 attempts to visit illegal child abuse sites every day.[149]

Cybertip.ca, run by the Canadian Centre for Child Protection,[150] operates a Canadian Cleanfeed project and provides a list of specific foreign-hosted Internet addresses associated with images of child sexual abuse to participating ISPs.[151] These ISPs then use the technology to filter or prevent access to those sites. On average, Cybertip.ca receives over 700 reports and 800,000 hits to its website per month. The reports have resulted in dozens of arrests, the eliminations of thousands of websites and the rescue of numerous children.

In Canada, some companies voluntarily participate in Project Cleanfeed to block foreign websites hosting prepubescent images.[152] Unlike the U.K., Canada's Cleanfeed targets

[148] Philip K. Reitinger, *Written Congressional Testimony—Making the Internet Safe for Kids: The Role of ISPs and Social Networking Sites*, June 27, 2006.
[149] BBC News, February 7, 2006.
[150] Canadian Centre for Child Protection, a charitable organization dedicated to the personal safety of all children.
[151] In the U.K., the Internet Watch Foundation provides the list.
[152] Cybertip reports domestic sites to Canadian law enforcement agencies.

only "prepubescent" material so that participating ISPs do not unintentionally block legal sites that include females over the age of 18 (many of whom are advertised as looking younger).[153]

As of February 2009, only eight of the more than 400 ISPs in Canada participated in Cleanfeed Canada.[154] Fortunately, most of the largest ISPs, such as Telus and Bell, do participate, which means that almost 90 percent of all Canadian Internet subscribers are covered by the Cleanfeed program. While those ISPs that are voluntarily participating should be congratulated, **every** ISP in Canada should be obligated to participate in this initiative.

Since 2006, there have been 13,000 URLs[155] added to Cybertip.ca's list. Almost half of these sites involve sexual acts with children and almost 90 percent involve children under 8.[156] One ISP identified 2,900 attempts in a 24-hour period to access a blocked website.[157] Despite these statistics, it is important to keep in mind that 80 percent of millions of sites still leaves hundreds of thousands accessible.

There are those who will argue that stricter laws or filters interfere with regular, legitimate sites. Cybertip.ca has addressed this by putting in place a thorough appeal process for someone who feels legal material has been blocked.

Furthermore, the potential negatives of having stronger filters or a more restrictive approach are generally limited to prohibiting access to a site that advertises adult females who look like they might be 12. Given the extensive appeal process, we do not believe this current limitation is justifiable.

RECOMMENDATION 9—That the federal government introduce legislation to require all ISPs to block access to sites containing images of children who are or are depicted as being under the age of 18 years, and block the distribution of known child sexual abuse images based on images collected by the National Child Exploitation Coordination Centre.

153 The U.K. list includes any site that contains potentially illegal child sexual abuse content that would be an offence to download (make).

154 www.cybertip.ca/app/en/cleanfeed_p2#anchor_menu.

155 A URL (Uniform Resource Locator) is the unique address for a file that is accessible on the Internet. For example, to get to a website, you can enter the URL of the home page in your Web browser's address line.

156 Signy Arnason, Cybertip.ca, Ontario Provincial Strategy to Protect Children from Sexual Abuse and Exploitation on the Internet Multi-disciplinary Conference, November 18, 2008, London, Ontario.

157 Noni Classen, Canada Centre for Child Protection, BOOST—Responding to Child & Youth Victims of Sexual Exploitation on the Internet Conference, Collingwood, Ontario, September 2007.

"We have an opportunity to stop the continual trauma experienced by victims of Internet-facilitated sexual abuse by treating these images as what they are—ongoing abuse."

THIS REPORT HAS IDENTIFIED A NUMBER OF SIZABLE GAPS where children are falling through the cracks and offenders are gaining momentum. *Each of these gaps represents an opportunity to act; to make positive change and to protect vulnerable children.*

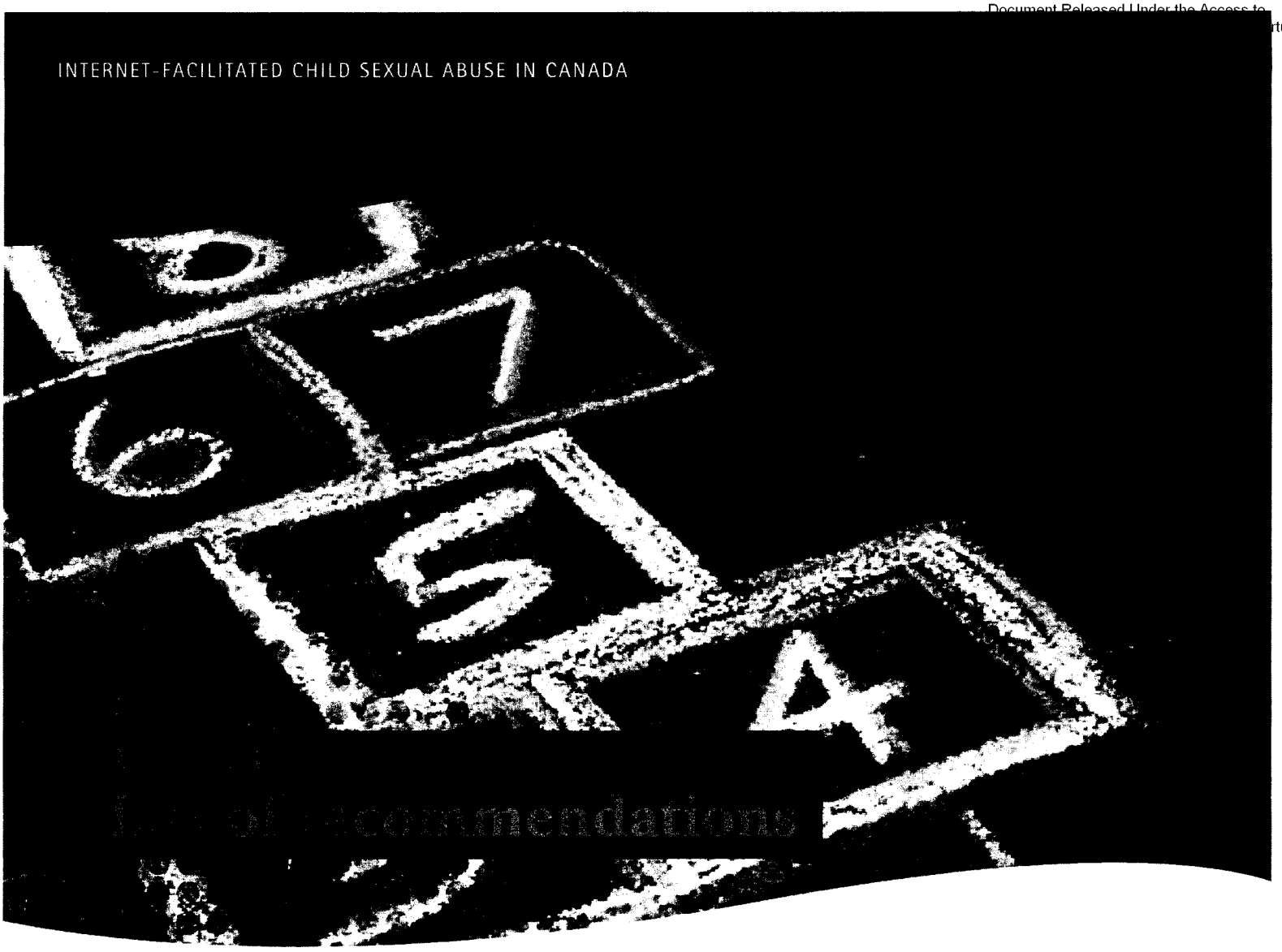
There is an opportunity to better communicate the horror of the problem by moving away from the term "child pornography" to more accurate terms such as "child sexual abuse images" or "child sexual abuse videos."

We have an opportunity to help dedicated law enforcement professionals more effectively find the offenders *and* victims of these abuses by giving them the tools they need to pursue investigations—including the ability to obtain simple customer name and address information, to access computers that have been seized regardless of password protections or encryptions, and to provide support and resources to finding better and more efficient ways to analyze images.

In cases where law enforcement is able to identify and rescue victims, there is an opportunity to make a difference in victims' lives by fostering a stronger understanding of their needs and responding with effective, victim-friendly services.

Finally, we have an opportunity to stop the continual trauma experienced by victims of Internet-facilitated sexual abuse by treating these images as what they are—ongoing abuse. By ceasing the disclosure of images and by making private sector ISPs more accountable, there is an opportunity to spare a child one more humiliation.

We request the Ministers of Justice, Public Safety and Industry and affected agencies to consider these opportunities and recommendations and to report back to the Office of the Federal Ombudsman for Victims of Crime. We look forward to the Government's action plan, detailing how it will move forward to enhance the protection of children.



Recommendation 1

That the federal government introduce legislation to amend the child pornography provisions in the *Criminal Code* to provide a more accurate description of the crime (i.e. such as child sexual abuse images, child sexual abuse videos, child sexual abuse writings) to ensure a more accurate reflection of the harm that is done to victims.

Recommendation 2

That the federal government expedite legislation to require ISPs to provide customer name and address information to law enforcement.

Recommendation 3

That the federal government introduce legislation to require ISPs to retain customer name and address data, traffic data and content data for two to five years.

Recommendation 4

That the federal government introduce legislation to amend the *Criminal Code* to make the refusal to provide a password or encryption code upon judicial order a criminal offence.

Recommendation 5

That the federal government, in partnership with the provinces, develop a national strategy to identify victims found in child sexual abuse images and that the strategy includes an expansion of the National Child Exploitation Coordination Centre's National Victim Identification Unit and support for the national image database.

Recommendation 6

That the federal government, in conjunction with provincial and municipal governments, develop a national strategy to expand the network of Child Advocacy Centre models in communities across the country.

Recommendation 7

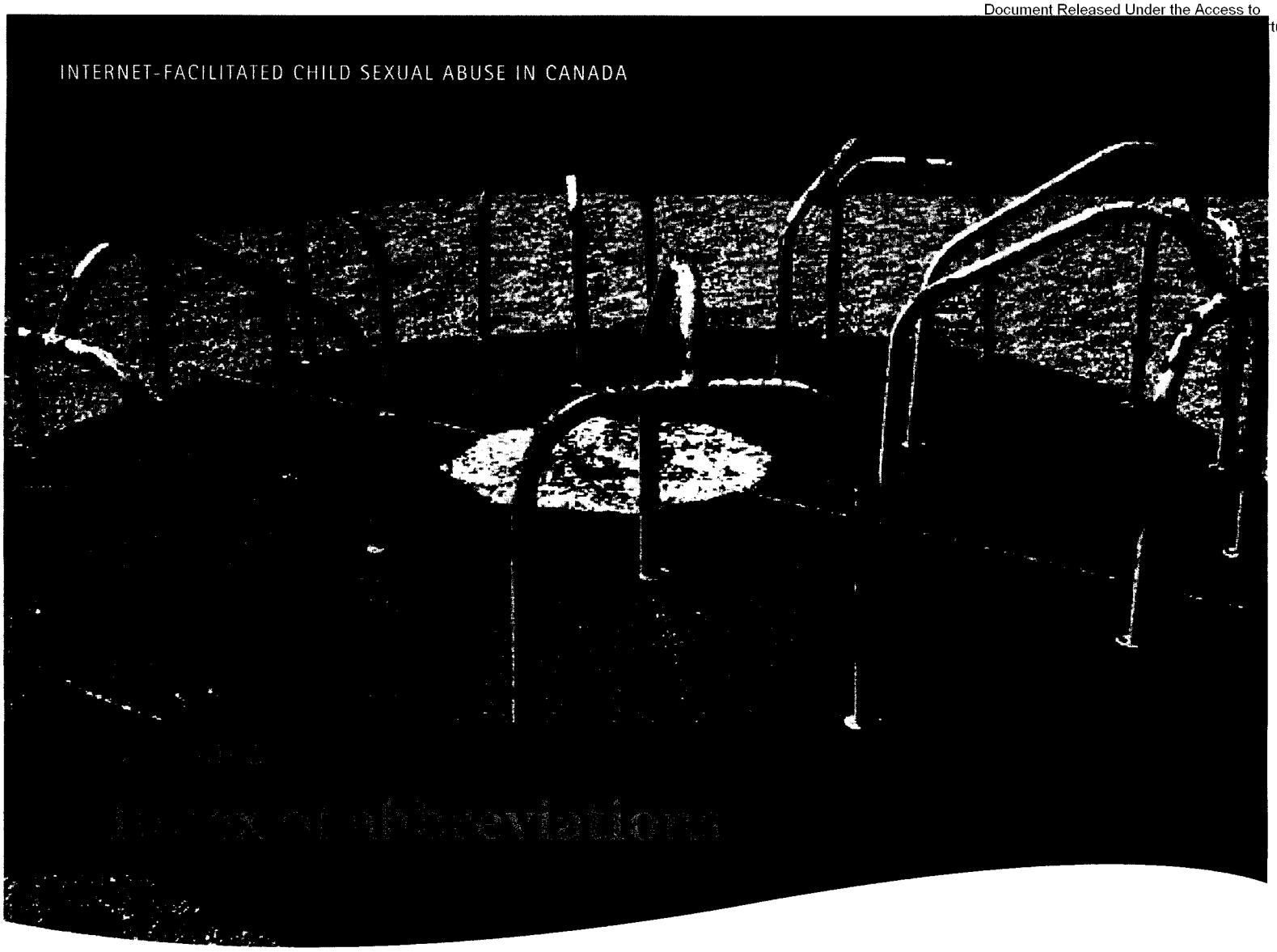
That the Department of Justice's Policy Centre for Victim Issues fund research into the needs of victims of Internet-facilitated child sexual abuse.

Recommendation 8

That the federal government introduce legislation to amend the *Criminal Code* to ensure that child sexual abuse images, video or audio recordings are not disclosed to defence counsel but that opportunities are made available for proper review of the evidence.

Recommendation 9

That the federal government introduce legislation to require all ISPs to block access to sites containing images of children who are or are depicted as being under the age of 18 years, and block the distribution of known child sexual abuse images based on images collected by the National Child Exploitation Coordination Centre.



List of abbreviations

CAC – Child Advocacy Centre

CCAICE – Canadian Coalition Against Child Exploitation

CEOP – Child Exploitation and Online Protection Centre

CNA – Customer Name and Address Information

FINTRAC – Financial Transactions and Reports Analysis Centre of Canada

ICAID – INTERPOL Child Abuse Image Database

ICE – Integrated Child Exploitation Team

IP – Internet Protocol

ISP – Internet Service Provider

KINSA – Kids Internet Safety Alliance

NCA – National Children's Alliance

NCECC – National Child Exploitation Coordination Centre

NCMEC – National Center for Missing and Exploited Children

OPP – Ontario Provincial Police

PIPEDA – *Personal Information Protection and Electronic Documents Act*

RCMP – Royal Canadian Mounted Police

CUSTOMER NAME AND ADDRESS CONSULTATIONS

Public Safety Canada

By: Canadian Resource Centre for Victims of Crime
October 10, 2007

Introduction

The Canadian Resource Centre for Victims of Crime (CRCVC) is a non-government, non-profit advocacy group for victims and survivors of violent crime. We provide direct assistance to victims across the country as well as advocate for more services and protections for victims and the public. We were pleased to receive an invitation from Public Safety Canada to participate in the consultation process regarding possible measures to address law enforcement and national security agencies' lawful access to customer name and address (CNA) information held by telecommunications service providers (TSPs).

As a non-government organization dedicated to ensuring the voice of victims and survivors is heard, we agree that the rights and freedoms guaranteed in the *Canadian Charter of Rights and Freedoms* must be protected. However, the protection of an individual's privacy cannot take precedence over the protection of the public from national security threats or the protection of children from sexual exploitation.

Canada is in no way immune to terrorist threats, as seen with the arrest of a Quebec man in connection with an online plot to bomb targets outside Canada on September 14, 2007. If not for the prompt response of the RCMP and other law enforcement groups, a serious incident may have occurred.

We have long advocated for increased protections for child victims; including those who may be sold, prostituted or used for child pornography. Our largest area of focus has been on advocating for increased resources for law enforcement to allow them to fully investigate and rescue children from sexual exploitation on the Internet.

As stated in the consultation document, law enforcement has repeatedly voiced their concerns about the difficulty in consistently obtaining basic CNA information in the course of their duties. Officials need prompt cooperation from TSPs in order to prevent threats to national security/public safety and to rescue abused children. It is our opinion that corporations should be obligated to assist law enforcement (without a warrant), as any good citizen would, in preventing and investigating crime.

Our position

In 2000, the CRCVC sent a discussion paper to all Members of Parliament and Senators entitled "Child Sexual Exploitation and the Internet." We made 20 recommendations, including that legal requirements be imposed on Internet Service Providers (ISPs) to cooperate with law enforcement, the creation of a new offence of luring, raising the age of consent, creation of a national tip-line, etc. It is unfortunate that seven years later, law enforcement agencies still face challenges accessing basic CNA information.

The lack of explicit legislation in this area gives telecommunications companies the discretion to provide information to law enforcement when it is requested or to demand a court order before releasing any information at all, regardless of the situation at hand. This is problematic at any stage of an investigation, likely halting it or creating significant delays while documents to compel the information are sought. We should not have to reiterate the risk of delays in the context of preventing terrorism or rescuing children from sexual abuse. We believe the government should immediately amend section 7(3) of the *Personal Information Protection and Electronic Documents Act (PIPEDA)* to make it clear that 'lawful authority' does not require a warrant in order to ensure the police and national security agencies are granted CNA information.

We fully support the use of safeguards, as listed in the consultation document. In order to prevent abuses, for example, we support limits on who can have access to the information, limiting how it is used, and internal audits on the use of the powers, etc. We agree that lawful access to CNA information should not include the content of communications or the web sites an individual visited online unless a court order is issued.

Concerns of privacy advocates

The problem of child pornography on the Internet is getting worse, and despite the many successes of Canadian law enforcement, police are only able to scratch the surface. We applaud the continued, difficult work of police officers in sorting through tens of thousands of images of child pornography in order to catch the predators and stop the abuse of children. Their objectives are simple – arrest those who create, distribute and access child pornography and identify and rescue those children who have already been harmed.

Some privacy advocates suggest, "Canadian law enforcement and national security agencies are looking for a quick and easy way to obtain access to the names, phone numbers, IP addresses,

etc...of customers of Canadian telecommunications service providers. Quick and easy, in this context, means without the delay and paperwork involved in applying to a judge for a search warrant."[1] We urge officials to remember that police/national security officials seek this information in a number of contexts, including in the very beginning of investigations or as part of intelligence gathering. We submit that persons who come to the attention of law enforcement or national security agencies in the course of their investigative duties are 'persons of interest'. Their actions online have raised serious red flags. We do not believe that CNA information is sought when there is insufficient evidence to connect an individual to a crime so that a judge would not issue a warrant, or so officials can go searching for crimes that may be occurring outside of the scope of their investigation.

Law enforcement and national security agencies must act quickly when such 'persons of interest' come to their attention. There is not always ample time to obtain lawful authority in the form of a warrant. Immediate threats to national security and the sexual abuse of children must override the protection of anyone's personal information by *PIPEDA*.

We urge Public Safety officials to remember the privacy violations of the innocent children whose images are being traded like baseball cards every day for the sexual satisfaction of pedophiles and predators. There is no greater violation of privacy then having images and videos of someone raping you distributed around the world. We cannot allow these crimes to continue to be facilitated by private companies in Canada who provide broadband Internet access, virtual storage areas for abuse images and anonymous e-mail, and forums for pedophiles to support each other in the belief that having sex with children is not wrong.

Tom Copeland, head of the Canadian Association of Internet Providers, has stated that requiring a search warrant for police to get a suspect's name and address is "over-kill" and that that information is not normally considered private. We agree, and would submit, that much of the "personal information" held by TSPs is already public information contained in most telephone directories.

We also submit that cooperation by TSPs on a case-by-case basis, which is what generally occurs now, is simply not good enough when it comes to the safety/protection of children or threats to

[1] David T.S. Fraser, "Some necessary background information to the fuss over warrant-less access to Canadian personal information," 15 September 2007. http://www.privacylawyer.ca/blog/2007/09/some-necessary-background-to-fuss-over.html

national security. Privacy advocates maintain that there must be court oversight in order to hand over personal information and that police investigations have not been hampered to date. However, investigations have been hampered, as reported by many police officers during the Statutory Review of *PIPEDA* in 2006/2007. In our opinion, police do not and should not need a warrant to secure subscriber information or in any other circumstance except when dictated by Parliament.

Police do not need a warrant to check a license plate in order to identify the owner of a vehicle that is suspected of being involved in a crime. There are many examples where law enforcement has access to information that the average citizen does not. They have access to this information because they are tasked with preventing and investigating crime and they have an already well established legal obligation not to disclose the information that they obtain except within the course of their mandated duties.

The Problem

As *PIPEDA* currently exists, it requires the consent of the individual for all collection, use and disclosure of personal information, subject to a number of exceptions. "Personal information" includes any information about an identifiable individual. It is thus illegal for TSPs to disclose such information without consent.

What constitutes *lawful authority* is at question. Subsection 7(3)(c) of the legislation is where the confusion occurs, as it sets out provisions where an organization may disclose personal information without consent. The first condition is when it is in compliance with a subpoena, warrant or court order. The second stipulation for disclosure is in response to a request by a government institution that has the *lawful authority* to obtain the personal information for the purpose of enforcing a law, carrying out an investigation related to the enforcement of the law, or gathering intelligence for purposes of enforcing a law.[2] The second condition should be treated independently of the first, yet in our meetings with law enforcement we have heard that TSPs tend to treat these two conditions as one. Thus, they are interpreting *lawful authority* to mean a warrant is always required.

[2] Section 7(3)(*c*.1) states that an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is "made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs, (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or (iii) the disclosure is requested for the purpose of administering any law of Canada or a province;"

On December 18, 2006, the Privacy Commissioner wrote the CRCVC and stated that under section 7(3)(c.1)(ii), "the decision to disclose the information rests with the organization…In other words, the disclosure is discretionary on the part of the organization." We submit, once again, that discretionary disclosure is simply unacceptable when it comes to public safety and the sexual exploitation of children.

CRCVC Recommendations

Given the confusion that exists regarding lawful authority and the hesitation of some TSPs to comply with law enforcement requests, we recommend (at the minimum) that section 7(3) be amended to make it clear 'lawful authority' does not mean a warrant is required. Lawful access to CNA information at the outset or during the course of an investigation should be clearly defined.

We further recommend an amendment, in the case of investigations involving child abuse/child pornography and threats to national security, to stipulate that TSPs shall cooperate with law enforcement.

Thank you for the opportunity to participate.

Respectfully submitted,

Heidi Illingworth
Executive Director

Willey, Chris

From: Willey, Chris
Sent: Tuesday, February 26, 2013 1:21 PM
To: McRae, Marley; Carta, John; Paulson, Erika
Cc: Picard, Josée; Communications_
Subject: RE: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

I'd suggest following up with National Security Technology on this. Maciek Hawrylak would likely be your best bet.

--
Chris Willey
Public Safety Canada | Sécurité publique Canada
Tel: (613) 949-9287 Fax: (613) 954-8435

From: McRae, Marley
Sent: Tuesday, February 26, 2013 1:00 PM
To: Carta, John; Paulson, Erika; Willey, Chris
Cc: Picard, Josée; Communications_
Subject: RE: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

Anyone know anything about this or who clients would be?

From: Communications_
Sent: Tuesday, February 26, 2013 12:55 PM
To: McRae, Marley
Cc: Communications_; Picard, Josée
Subject: Public enquiry re: Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications

Hello Marley,

Would you know where we might be able to retrieve a copy of the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications?
We would appreciate any direction you could provide, thank you.

Name	[redacted]
Enquiry Date	2/14/2013
Language	English
Phone #	s.19(1)
Location	Ontario
E-mail	[redacted]@gmail.com
Type of Enquiry	Related to Public Safety
Method of Enquiry	E-mail
Organization	
PS Branch	
Program	
Portfolio Agency/Review Bodies	

Questions

Hello,
I would like to obtain a copy of the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications, along with any proposed changes.
It says at
http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10473.html
" For further information on proposed changes to the Solicitor General's Enforcement Standards, please contact Public Safety Canada via the General Enquiries line at 1-800-830-3118."
I decided to try to contact you by electronic means first but will telephone if necessary.

Zarah Malik

Agente des communications | Communications Officer
Gestion des enjeux, Affaires publiques | Issues Management Team, Public Affairs Division
Ministère de la sécurité publique | Department of Public Safety
T : 613-949-5536 | F : 613-954-4779

Durand, Stéphanie

From: Greg Cox <Greg.Cox@rcmp-grc.gc.ca>
Sent: Tuesday, January 15, 2013 2:43 PM
To: Swift, Andrew; Wilson, Barbara; Slack, Jessica
Cc: Durand, Stéphanie; Lavoie, Daniel; Derek Cefaloni; Julie Gagnon; Marc Richer
Subject: Re: Reader's Digest Interview Request

First off, It is a production order that is required, not a warrant so not sure why that was changed.....

Will read it over...

Greg

Sgt. Greg Cox
RCMP Media Relations
613-843-5999
-----Original Message-----
From: "Slack, Jessica" <Jessica.Slack@ps-sp.gc.ca>
Cc: Richer, Marc <Marc.Richer@rcmp-grc.gc.ca>
Cc: Gagnon, Julie <julie.gagnon@rcmp-grc.gc.ca>
Cc: Lavoie, Daniel <Daniel.Lavoie@rcmp-grc.gc.ca>
To: Cox, Greg <Greg.Cox@rcmp-grc.gc.ca>
Cc: Cefaloni, Derek <Derek.Cefaloni@rcmp-grc.gc.ca>
To: Swift, Andrew <Andrew.Swift@ps-sp.gc.ca>
To: Wilson, Barbara <Barbara.Wilson@ps-sp.gc.ca>
Cc: <Stephanie.Durand@ps-sp.gc.ca>

Sent: 01/15/2013 14:36:25
Subject: RE: Reader's Digest Interview Request

Hi Greg – some requested changes from Public Safety... Sorry for the delay!
Thanks,
Jessica
IP addresses, email addresses, and other electronic identifiers are key pieces of evidence in investigations of cyber-crimes. It is rare that a suspect name is provided at the beginning of an investigation.
In order to begin an investigation and determine the jurisdiction, the police requires the name and address of the account holder of the IP address which committed the offence. It is important to note that the account holder is not necessarily the person who committed the offence.
Obtaining the name and address of the account holder is simply a starting point to an investigation and crucial in assessing risk factors. The name and address information requested by the police can be obtained without a warrant, when the ISP consents to release this information.
If the police require access to content (i.e. browsing history, downloads, etc.) a warrant is required by law.

From: Swift, Andrew
Sent: January-14-13 5:58 PM
To: 'Greg Cox'; Wilson, Barbara; Slack, Jessica
Cc: Durand, Stéphanie; Lavoie, Daniel; Derek Cefaloni; Julie Gagnon; Marc Richer
Subject: RE: Reader's Digest Interview Request

Thanks Greg. We will consult internally and get back to you tomorrow.
Andrew
From: Greg Cox [mailto:Greg.Cox@rcmp-grc.gc.ca]
Sent: Monday, January 14, 2013 5:09 PM
To: Swift, Andrew; Wilson, Barbara; Slack, Jessica
Cc: Durand, Stéphanie; Lavoie, Daniel; Derek Cefaloni; Julie Gagnon; Marc Richer
Subject: Fwd: Reader's Digest Interview Request

[redacted] Reader's Digest asked the following. Below is our proposed response. s.19(1)

My questions deal with cyber crime, particularly Internet predators, and what the RCMP does and does not have the right to do when investigating online offenders. I'm also trying to get my head around the issue of lawful access, something that came into the spotlight last year when the federal government tabled Bill C-30. I don't fully understand lawful access and could use some help.
Would somebody be able to chat to me early next week about these issues? My questions are pasted below.
My understanding is that, when police want to attain the personal information of a person whose IP address they already know, they can ask the person's Internet service provider (ISP) for that information. The ISP has the option of either granting or refusing the request; however, in cases where the ISP refuses such a request, the RCMP can serve them with a warrant, provided there is sufficient justification for doing so. Am I correct here?

Last year, the Canadian government tabled Bill C-30, which, had it passed, would have given the police broader powers when investigating Internet predators. Currently, the RCMP has the right to request personal information about Internet users from Internet service providers. But the Internet service providers can decline these request, in which case the RCMP must produce a warrant if they are to attain the information they seek. As I understand it, Bill C30 would have done away with the warrant process. Had the bill passed, it would have enabled the police to request personal information from ISPs, and ISPs would have been obliged to comply with those request, even in cases where a warrant wasn't presented. Am I correct here?
Right now, I don't have a sense as to why a lawful access law like Bill C-30 would help police officers in their investigative duties. Can somebody in the RCMP help me out here? Why do people within our government feel that the warrant system needs to be amended? Does the warrant system prevent the police from effectively investigating Internet predators?
What's the police protocol for monitoring cyber crime? I had imagined that police spend time trawling online forums and image boards where illicit material (like child pornography) circulates. I had imaged that when police find something suspicious, they then see about obtaining the personal information of the people involved by contacting ISPs. Am I broadly correct here?

Are there any technologies that enable the police to monitor the activities of online predators? The Internet is a large domain? How does the RCMP keep on top the plethora of illicit activities that go on in Cyberspace?
****
Our response:
Child pornography investigations are based on IP addresses, usernames and/or emails. It is rare that a suspect name is provided at the beginning of an investigation.

In order to begin an investigation and determine the jurisdiction, the police require the name and address of the account holder of the IP address which committed the offence. It is important to note that the account holder is not necessarily the person who committed the offence.

Obtaining the name and address of the account holder is simply a starting point to an investigation and crucial in assessing risk factors. Without this information, an investigation cannot commence. The name and address information requested by the police can be obtained without a warrant. This is common information, no different than utilizing a phone book.

If the police require more information on the account, (ie: emails, where the IP has surfed online etc) a production order is required by law.
For all questions related to C-30, you will need to contact Public Safety.

Willey, Chris

From: Paulson, Erika
Sent: Wednesday, January 09, 2013 1:58 PM
To: Willey, Chris; Austria, Jamela
Subject: Canadian Privacy Law Blog: Privacy Commissioner proposes lawful access compromise

http://blog.privacylawyer.ca/2013/01/privacy-czar-tries-to-broker-internet.html

Seen this?

Bue, Richard

From: Durand, Stéphanie
Sent: Thursday, January 03, 2013 2:01 PM
To: Duval, Jean Paul
Cc: Filipps, Lisa; Swift, Andrew; Wilson, Barbara; Bue, Richard
Subject: RE: For approval: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Fine by me. Thx

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Duval, Jean Paul
Sent: Thursday, January 03, 2013 1:58 PM
To: Durand, Stéphanie
Cc: Filipps, Lisa; Swift, Andrew; Wilson, Barbara; Bue, Richard
Subject: For approval: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Stéphanie,

For your approval, here is the proposed response to the Globe and Mail request on the *Solicitor General Enforcement Standards for Lawful Interception of Telecommunications*. We have shared with IC and do not expect any concerns to be raised.

Approved by:
Mike MacDonald
Andrew Swift

Proposed response:

- We respectfully decline your request for an interview and would note that the document entitled *Solicitor General Enforcement Standards for Lawful Interception of Telecommunications,* is provided to radio and spectrum licence holders to assist them in complying with their lawful interception condition of licence. This document contains sensitive content and is not publicly available.

Regards,
JP

Title [redacted] **s.19(1)**

Media Outlet	Globe and Mail
Call Date	12/31/2012 3:00 PM
Telephone	
E-mail address	@globeandmail.com
Deadline	
Status	Consulting
Branch	NS
Subject	Lawful Interception Enforcement Standards (re:Lawful Access)
Questions	I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008. I am seeking a discussion with someone in the division to discuss these specific 22 measures. Would that be possible? Document info: - "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table." - said to be "current as of Nov. 17 2008" - 22 standards make explicit what the government is seeking from telecom networks and carriers - Annotated with italics further explaining the standards - Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc) - Prepared by Public Safety's National Security Technology Division

s.19(1)

Jean Paul Duval
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-1689
Cell | Portable:
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

Carignan, Joëlle

From: Mueller, Mike
Sent: Monday, December 31, 2012 3:24 PM
To: Duval, Jean Paul; Carmichael, Julie; McGrath, Andrew; Johnson, Mark
Cc: Tomlinson, Jamie; Miller, Kevin; Champoux, Martin
Subject: Re: Notification: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Can you please provide me with a copy of the document "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications"?

Thanks

Mike

From: Duval, Jean Paul
Sent: Monday, December 31, 2012 03:18 PM
To: Carmichael, Julie; McGrath, Andrew; Johnson, Mark; Mueller, Mike
Cc: Tomlinson, Jamie; Miller, Kevin; Champoux, Martin
Subject: Notification: Media Call - Globe and Mail - Lawful Interception Enforcement Standards

Julie,

We received a request from the Globe and Mail seeking an interview/discussion on specific interception standards for telecommunication carriers as detailed in the "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications".

We are consulting.

Regards,
JP

Title		[redacted]
Media Outlet		Globe and Mail
Call Date	s.19(1)	12/31/2012 3:00 PM
Telephone		[redacted]
E-mail address		[redacted]@globeandmail.com
Deadline		Open
Status		Consulting
Subject		Lawful Interception Enforcement Standards (re: Lawful Access)
Questions		I am reviewing a document put together by Public Safety Canada's National Security Technology Division regarding 22 specific interception standards that telecom carriers were asked to provide police circa 2008. I am seeking a discussion with someone in the

division to discuss these specific 22 measures. Would that be possible?

Document info:
- "Solicitor General's Enforcement Standards for the Lawful Interception of Telecommunications -- Compliance Table."
- said to be "current as of Nov. 17 2008"
- 22 standards make explicit what the government is seeking from telecom networks and carriers
- Annotated with italics further explaining the standards
- Among measures made explicit are needs for intercepting various modalities (call forwarding / real-time audio / data-voice correlation accuracy measures / encryption algorithms, etc etc etc)
- Prepared by Public Safety's National Security Technology Division

Jean Paul Duval
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-1689
Cell | Portable: [redacted]
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

s.19(1)

Durand, Stéphanie

From: Durand, Stéphanie
Sent: Friday, October 26, 2012 3:05 PM
To: Swift, Andrew
Subject: Re: CACP Bill C-30 / Lawful Access

Good - thx

From: Swift, Andrew
Sent: Friday, October 26, 2012 02:49 PM
To: Durand, Stéphanie
Subject: FW: CACP Bill C-30 / Lawful Access

I've shared with Mike Macdonald as well.

Andrew Swift

Director, Public Affairs | Directeur, Affaires publiques
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-3549
Fax | Télécopieur : 613-954-2000
Email | Courriel : Andrew.Swift@ps-sp.gc.ca

From: Swift, Andrew
Sent: Friday, October 26, 2012 2:48 PM
To: Carmichael, Julie; Johnson, Mark; Mueller, Mike; McGrath, Andrew
Cc: Durand, Stephanie; Carta, John; Wilson, Barbara
Subject: FYI: CACP Bill C-30 / Lawful Access

Julie,
Here's the pick-up thus far on the CACP news conference today re. C-30, including social media. We will continue to monitor. We haven't received any calls so far.
Andrew

Vancouver police chief backs maligned Internet surveillance bill
October 26, 2012, 13:59 ET
Globe and Mail, By: Andrea Woo

Vancouver's police chief is urging the federal government to pass Bill C-30, the controversial Internet surveillance bill.

Chief Jim Chu, who is also President of the Canadian Association of Chiefs of Police, told a news conference in Vancouver police are handcuffed by outdated laws, particularly in situations involving kidnappings, fraud and cyberbullying.

Chief Chu's appeal comes in the aftermath of the suicide of B.C. teen Amanda Todd, who took her own life on Oct. 10 after relentless bullying online and in person.

The controversial bill, introduced by Stephen Harper's Conservative government in February, would grant law enforcement agencies and the federal government the power to obtain identifying information on Canadians online without having to apply for a warrant.

Critics had scoffed at the bill – also called the "Protecting Children from Internet Predators Act" or the lawful access legislation – and Public Safety Minister Vic Toews' remark that those who opposed the legislation stood "with the child pornographers."

Amid the opposition, the federal government said it would review the bill, but months have passed and it since appears to have died.

More to come

Link

News Releases

Media Release - CACP Renews Appeal for Lawful Access Legislation / Communique - L'ACCP réitère son appel à l'action en faveur de mesures législatives sur l'accès légal
Link

Halifax Regional Police Supports CACP Position on Lawful Access
Link

Social Media search

AndreaWoo1:08pm via Echofon
Chu: Strong stance needed to prevent, investigate serious crimes like kidnappings, fraud. Handcuffed by outdated laws. pic.twitter.com/LkfkGwqc

AndreaWoo1:08pm via Echofon
Chu: Cyber bullying very concerning. Bill needed to prevent further tragedies.

AndreaWoo1:10pm via Echofon
Chu: some wording in bill needs to be change so authorities won't get "unfettered access."

AndreaWoo1:13pm via Echofon
Now watching vid. If person was attacked by someone who dropped cell phone, telecommunication company not legally required to provide ID

AndreaWoo1:22pm via Echofon
Dept Police Chief Warren Lemcke: Bill C-30 would approve accountability because only certain ppl can request, will be on record

AndreaWoo1:29pm via Echofon
Chu: Can't just access records for anyone w/o proper grounds.

AndreaWoo1:32pm via Echofon
Chu: There are criminal sanctions for anyone who violates lawful access rules, just like with paper records.

AndreaWoo1:44pm via Echofon
Lemcke: Bill C-30: Can access name, address, phone number, IP address. Can't access emails, surfing habits, texts, etc

AndreaWoo1:45pm via Echofon
Lemcke: "Internet surveillance bill" bit of misnomer because we can't do any surveillance without warrant

AndreaWoo1:52pm via Echofon
That's it for the news conference. Will update file shortly.

VancouverPD1:24pm via HootSuite
#VPD supports the #CACP on bill C-30. ow.ly/eNArH Video: ow.ly/eNAJz "Police Confirm Top 5 Fears about Lawful Access."

HfxRegPolice1:48pm via HootSuite
Earlier today, CACP issued a news release about lawful access. Chief Blais supports the position of the CACP - ow.ly/eNCkt WM

timsmith20001:45pm via Twitter for iPad
Bill C-30 - Chief CHU asked "What do you think about warrantless Internet spying?" "I am against it!" visit cacp.ca #cdnpoli

Dave_Eby1:27pm via HootSuite
Why won't police recognize lack of public support for warrantless internet spying? MT @VancouverPD: #VPD supports the #CACP on bill C-30.

CBCDonnelly1:23pm via Twitter for BlackBerry®
VPD chief says passage of Bill C-30 will give police ability to get cell phone and internet info from tele com providers #cbcdonnelly

Carignan, Joëlle

From: Despard, Sean
Sent: Friday, October 26, 2012 2:41 PM
To: Swift, Andrew; * Media Monitoring / Suivi des médias
Subject: CACP Bill C-30 / Lawful Access

Article (was included in 2pm package):

Vancouver police chief backs maligned Internet surveillance bill
October 26, 2012, 13:59 ET
Globe and Mail, By: Andrea Woo

Vancouver's police chief is urging the federal government to pass Bill C-30, the controversial Internet surveillance bill.

Chief Jim Chu, who is also President of the Canadian Association of Chiefs of Police, told a news conference in Vancouver police are handcuffed by outdated laws, particularly in situations involving kidnappings, fraud and cyberbullying.

Chief Chu's appeal comes in the aftermath of the suicide of B.C. teen Amanda Todd, who took her own life on Oct. 10 after relentless bullying online and in person.

The controversial bill, introduced by Stephen Harper's Conservative government in February, would grant law enforcement agencies and the federal government the power to obtain identifying information on Canadians online without having to apply for a warrant.

Critics had scoffed at the bill – also called the "Protecting Children from Internet Predators Act" or the lawful access legislation – and Public Safety Minister Vic Toews' remark that those who opposed the legislation stood "with the child pornographers."

Amid the opposition, the federal government said it would review the bill, but months have passed and it since appears to have died.

More to come

Link

News Releases

Media Release - CACP Renews Appeal for Lawful Access Legislation / Communique - L'ACCP réitère son appel à l'action en faveur de mesures législatives sur l'accès légal
Link

Halifax Regional Police Supports CACP Position on Lawful Access
Link

Social Media search

AndreaWoo1:08pm via Echofon
Chu: Strong stance needed to prevent, investigate serious crimes like kidnappings, fraud. Handcuffed by outdated laws. pic.twitter.com/LkfkGwqc

AndreaWoo1:08pm via Echofon
Chu: Cyber bullying very concerning. Bill needed to prevent further tragedies.

AndreaWoo1:10pm via Echofon
Chu: some wording in bill needs to be change so authorities won't get "unfettered access."

AndreaWoo1:13pm via Echofon
Now watching vid. If person was attacked by someone who dropped cell phone, telecommunication company not legally required to provide ID

AndreaWoo1:22pm via Echofon
Dept Police Chief Warren Lemcke: Bill C-30 would approve accountability because only certain ppl can request, will be on record

AndreaWoo1:29pm via Echofon
Chu: Can't just access records for anyone w/o proper grounds.

AndreaWoo1:32pm via Echofon
Chu: There are criminal sanctions for anyone who violates lawful access rules, just like with paper records.

AndreaWoo1:44pm via Echofon
Lemcke: Bill C-30: Can access name, address, phone number, IP address. Can't access emails, surfing habits, texts, etc

AndreaWoo1:45pm via Echofon
Lemcke: "Internet surveillance bill" bit of misnomer because we can't do any surveillance without warrant

AndreaWoo1:52pm via Echofon
That's it for the news conference. Will update file shortly.

VancouverPD1:24pm via HootSuite
#VPD supports the #CACP on bill C-30. ow.ly/eNArH Video: ow.ly/eNAJz "Police Confirm Top 5 Fears about Lawful Access."

HfxRegPolice1:48pm via HootSuite
Earlier today, CACP issued a news release about lawful access. Chief Blais supports the position of the CACP - ow.ly/eNCkt WM

timsmith20001:45pm via Twitter for iPad
Bill C-30 - Chief CHU asked "What do you think about warrantless Internet spying?" "I am against it!" visit cacp.ca #cdnpoli

Dave_Eby1:27pm via HootSuite
Why won't police recognize lack of public support for warrantless internet spying? MT @VancouverPD: #VPD supports the #CACP on bill C-30.

CBCDonnelly1:23pm via Twitter for BlackBerry®
VPD chief says passage of Bill C-30 will give police ability to get cell phone and internet info from tele com providers #cbcdonnelly

Durand, Stéphanie

From: Durand, Stéphanie
Sent: Wednesday, October 24, 2012 2:47 PM
To: Carmichael, Julie; Allison, Catherine
Cc: Swift, Andrew; Carta, John
Subject: Re: CACP to renew media campaign re. lawful access

RCMP is not having a representative participate in the press conference.

From: Carmichael, Julie
Sent: Wednesday, October 24, 2012 01:26 PM
To: Allison, Catherine
Cc: Durand, Stéphanie; Swift, Andrew; Carta, John
Subject: RE: CACP to renew media campaign re. lawful access

Thanks Cathy –

RCMP will not be participating, correct?

From: Allison, Catherine
Sent: October-24-12 1:25 PM
To: Carmichael, Julie
Cc: Durand, Stéphanie; Swift, Andrew; Carta, John
Subject: FW: CACP to renew media campaign re. lawful access
Importance: High

Hi Julie,

FYI below – realize the original email went to MO but thought I'd flip it to you as well just in case since you weren't on the dist. list.

Cathy

From: Carta, John
Sent: Wednesday, October 24, 2012 1:15 PM
To: Allison, Catherine; Swift, Andrew; Filipps, Lisa; Austria, Jamela; Willey, Chris
Subject: FW: CACP to renew media campaign re. lawful access
Importance: High

FYI – CACP to hold press conference on Oct 26 in support of lawful access leg.

From: MacDonald, Michael
Sent: October-24-12 1:12 PM
To: Durand, Stéphanie
Cc: Carta, John; Chayer, Marie-Helene
Subject: FW: CACP to renew media campaign re. lawful access
Importance: High

FYI

From: Timothy Smith [mailto:timsmith2000@rogers.com]
Sent: October-24-12 1:09 PM
To: MacDonald, Michael
Subject: Fwd: CACP to renew media campaign re. lawful access
Importance: High

Michael, lots happening since our last call. Wanted to ensure you were in the loop. Press Conf this Friday at 1:00 p.m.

Tim

Begin forwarded message:

From: Timothy Smith <timsmith2000@rogers.com>
Subject: CACP to renew media campaign re. lawful access
Date: 22 October, 2012 3:46:20 PM EDT
To: Tom.Jarmyn@ps-sp.gc.ca, Mike Mueller <Mike.Mueller@ps-sp.gc.ca>
Cc: Andrew House <andrew.house@ps-sp.gc.ca>, "julie.vaux@pmo.cpm.gc.ca" <julie.vaux@pmo.cpm.gc.ca>, "Timothy M. Smith" <timsmith2000@rogers.com>

As I know you are aware, the CACP has endorsed action on the issue of lawful access since 2002. We have made numerous presentations to speak to the need for new legislation that balances community safety and the privacy rights of all Canadians. The Act was introduced for first reading by the government on February 14, 2012 and we were extraordinarily supportive with the introduction including national, regional and local media conferences held by Chiefs across the country. We have kept you informed regarding discussions with the Office of the Privacy Commissioner of Canada. It is, however, obvious that we are not receiving positive signals regarding the future of this Bill, in particular, the need for Basic Subscriber Information.

Having reviewed the current status of this legislation, the importance of this bill to law enforcement and the efforts made by the CACP on this issue over the past many years, our Executive has directed an aggressive re-launch to media. It will begin on Friday, October 26 with a press conference in Vancouver held by Chief Constable Jim Chu and it will be followed by further information and regional / local media events by associated police leaders.

The purpose of my message was to keep you informed as to our work in this area and ensure that you were not caught off-guard. We had mentioned that we were producing a video as part of this campaign which is currently being translated and receiving final editing. It will be available to you coinciding with the press conference but is basically police leaders addressing misinformation surrounding lawful access.

Please let me know if you have any questions.

Tim

Timothy M. Smith
Government Relations and Strategic Communications,
Canadian Association of Chiefs of Police
www.CACP.ca

613-601-0692
timsmith2000@rogers.com

Durand, Stéphanie

From: Durand, Stéphanie
Sent: Wednesday, October 24, 2012 2:29 PM
To: Allison, Catherine
Subject: FW: CACP to renew media campaign re. lawful access

FYI – Daniel called on other issue.
I asked him to confirm as well.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | *Gouvernement du Canada*

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Carmichael, Julie
Sent: Wednesday, October 24, 2012 1:26 PM
To: Allison, Catherine
Cc: Durand, Stéphanie; Swift, Andrew; Carta, John
Subject: RE: CACP to renew media campaign re. lawful access

Thanks Cathy –

RCMP will not be participating, correct?

From: Allison, Catherine
Sent: October-24-12 1:25 PM
To: Carmichael, Julie
Cc: Durand, Stéphanie; Swift, Andrew; Carta, John
Subject: FW: CACP to renew media campaign re. lawful access
Importance: High

Hi Julie,

FYI below – realize the original email went to MO but thought I'd flip it to you as well just in case since you weren't on the dist. list.

Cathy

From: Carta, John
Sent: Wednesday, October 24, 2012 1:15 PM
To: Allison, Catherine; Swift, Andrew; Filipps, Lisa; Austria, Jamela; Willey, Chris

Subject: FW: CACP to renew media campaign re. lawful access
Importance: High

FYI – CACP to hold press conference on Oct 26 in support of lawful access leg.

From: MacDonald, Michael
Sent: October-24-12 1:12 PM
To: Durand, Stéphanie
Cc: Carta, John; Chayer, Marie-Helene
Subject: FW: CACP to renew media campaign re. lawful access
Importance: High

FYI

From: Timothy Smith [mailto:timsmith2000@rogers.com]
Sent: October-24-12 1:09 PM
To: MacDonald, Michael
Subject: Fwd: CACP to renew media campaign re. lawful access
Importance: High

Michael, lots happening since our last call. Wanted to ensure you were in the loop. Press Conf this Friday at 1:00 p.m.

Tim

Begin forwarded message:

From: Timothy Smith <timsmith2000@rogers.com>
Subject: CACP to renew media campaign re. lawful access
Date: 22 October, 2012 3:46:20 PM EDT
To: Tom.Jarmyn@ps-sp.gc.ca, Mike Mueller <Mike.Mueller@ps-sp.gc.ca>
Cc: Andrew House <andrew.house@ps-sp.gc.ca>, "julie.vaux@pmo.cpm.gc.ca" <julie.vaux@pmo.cpm.gc.ca>, "Timothy M. Smith" <timsmith2000@rogers.com>

As I know you are aware, the CACP has endorsed action on the issue of lawful access since 2002. We have made numerous presentations to speak to the need for new legislation that balances community safety and the privacy rights of all Canadians. The Act was introduced for first reading by the government on February 14, 2012 and we were extraordinarily supportive with the introduction including national, regional and local media conferences held by Chiefs across the country. We have kept you informed regarding discussions with the Office of the Privacy Commissioner of Canada. It is, however, obvious that we are not receiving positive signals regarding the future of this Bill, in particular, the need for Basic Subscriber Information.

Having reviewed the current status of this legislation, the importance of this bill to law enforcement and the efforts made by the CACP on this issue over the past many years, our Executive has directed an aggressive re-launch to media. It will begin on Friday, October 26 with a press conference in Vancouver held by Chief Constable Jim Chu and it will be followed by further information and regional / local media events by associated police leaders.

The purpose of my message was to keep you informed as to our work in this area and ensure that you were not caught off-guard. We had mentioned that we were producing a video as part of this campaign which is currently

being translated and receiving final editing. It will be available to you coinciding with the press conference but is basically police leaders addressing misinformation surrounding lawful access.

Please let me know if you have any questions.

Tim

Timothy M. Smith
Government Relations and Strategic Communications,
Canadian Association of Chiefs of Police
www.CACP.ca
613-601-0692
timsmith2000@rogers.com

Durand, Stéphanie

From: Allison, Catherine
Sent: Wednesday, October 24, 2012 1:17 PM
To: Durand, Stéphanie
Cc: Swift, Andrew
Subject: FW: CACP to renew media campaign re. lawful access

Importance: High

FYI – I see it went to MO directly from Rogers so I can make sure Julie is aware as well.

Cathy

From: Carta, John
Sent: Wednesday, October 24, 2012 1:15 PM
To: Allison, Catherine; Swift, Andrew; Filipps, Lisa; Austria, Jamela; Willey, Chris
Subject: FW: CACP to renew media campaign re. lawful access
Importance: High

FYI – CACP to hold press conference on Oct 26 in support of lawful access leg.

From: MacDonald, Michael
Sent: October-24-12 1:12 PM
To: Durand, Stéphanie
Cc: Carta, John; Chayer, Marie-Helene
Subject: FW: CACP to renew media campaign re. lawful access
Importance: High

FYI

From: Timothy Smith [mailto:timsmith2000@rogers.com]
Sent: October-24-12 1:09 PM
To: MacDonald, Michael
Subject: Fwd: CACP to renew media campaign re. lawful access
Importance: High

Michael, lots happening since our last call. Wanted to ensure you were in the loop. Press Conf this Friday at 1:00 p.m.

Tim

Begin forwarded message:

From: Timothy Smith <timsmith2000@rogers.com>
Subject: CACP to renew media campaign re. lawful access
Date: 22 October, 2012 3:46:20 PM EDT
To: Tom.Jarmyn@ps-sp.gc.ca, Mike Mueller <Mike.Mueller@ps-sp.gc.ca>

Cc: Andrew House <andrew.house@ps-sp.gc.ca>, "julie.vaux@pmo.cpm.gc.ca" <julie.vaux@pmo.cpm.gc.ca>, "Timothy M. Smith" <timsmith2000@rogers.com>

As I know you are aware, the CACP has endorsed action on the issue of lawful access since 2002. We have made numerous presentations to speak to the need for new legislation that balances community safety and the privacy rights of all Canadians. The Act was introduced for first reading by the government on February 14, 2012 and we were extraordinarily supportive with the introduction including national, regional and local media conferences held by Chiefs across the country. We have kept you informed regarding discussions with the Office of the Privacy Commissioner of Canada. It is, however, obvious that we are not receiving positive signals regarding the future of this Bill, in particular, the need for Basic Subscriber Information.

Having reviewed the current status of this legislation, the importance of this bill to law enforcement and the efforts made by the CACP on this issue over the past many years, our Executive has directed an aggressive re-launch to media. It will begin on Friday, October 26 with a press conference in Vancouver held by Chief Constable Jim Chu and it will be followed by further information and regional / local media events by associated police leaders.

The purpose of my message was to keep you informed as to our work in this area and ensure that you were not caught off-guard. We had mentioned that we were producing a video as part of this campaign which is currently being translated and receiving final editing. It will be available to you coinciding with the press conference but is basically police leaders addressing misinformation surrounding lawful access.

Please let me know if you have any questions.

Tim

Timothy M. Smith
Government Relations and Strategic Communications,
Canadian Association of Chiefs of Police
www.CACP.ca
613-601-0692
timsmith2000@rogers.com

Willey, Chris

From: Willey, Chris
Sent: Friday, October 05, 2012 4:13 PM
To: Carta, John
Subject: RE: lawful access
Attachments: Media Snapshot: Protecting Children from Internet Predators Act / Loi sur la protection des enfants contre les cyberprédateurs, 15-02-2012; Media Snapshot: Protecting Children from Internet Predators Act / Loi sur la protection des enfants contre les cyberprédateurs, 14-02-2012; PEA - Bill C-30 - 2012-02-14 - 2012-08-28.doc

---
Chris Willey
Public Safety Canada | Sécurité publique Canada
Tel: (613) 949-9287 Fax: (613) 954-8435

From: Carta, John
Sent: Friday, October 05, 2012 4:07 PM
To: Willey, Chris
Subject: lawful access

Do we have the package of PEA stuff on hand that Jamela gave to Joanne D?

John Carta
Communications - National Security / Sécurité nationale
Public Safety Canada / Sécurité publique Canada
Tel: 613.991.2701
John.Carta@ps-sp.gc.ca

Public Environment Analysis
Bill C-30
February 14, 2012 – August 28, 2012

Print / Online Media Overview

Print and online media coverage of Bill C-30 from February 14, 2012 – August 28, 2012 has been extensive with approximately 301 articles making mention of the subject. The tone of the coverage has been predominantly negative. ***NOTE: For detailed coverage of the announcement itself, please see the attached two snapshots.***

Critics of the bill state that it is overly intrusive, specifically provisions, which according to media would allow police to monitor the online activity of individuals via telecommunication companies with a warrant and would allow police to access internet subscribers' information (such as names, addresses, e-mail addresses, etc.) without a warrant.

Public Safety Minister Vic Toews addressed these concerns stating that ***"[t]here is nothing in the bill that would allow police to snoop on an individual's private conversations or even follow a person's activities on the Web. All that has to be done through a judicially authorized warrant***," and ***"[w]e also reduced the number of basic subscriber information points that police could request of service providers – the modern equivalent of phone book information – from 11 down to six***," (*Globe and Mail*, 2012-02-15, A6; *Telegraph-Journal*, 2012-02-29, A5). The need for a warrant to monitor online activity was reiterated by Warren Lemcke, Vancouver police Deputy Chief and co-chair of the Canadian Association of Chiefs of Police Law Amendments Committee, who stated, "One of the most important things to remember is this bill does not allow the police to monitor phone calls, emails or internet surfing without a warrant," (*Vancouver Sun*, 2012-02-21, A3). A similar response was provided by the Canadian Association of Chiefs of Police through a news release titled "Simplifying Access – Bill C-30 – Through the Lens of Law Enforcement". It states that "[d]ata or content of transmissions can only be released to law enforcement through a court-ordered warrant process...the legislation does not change this," (*Winnipeg Free Press*, 2012-02-25, A4).

In late February, shortly after Bill C-30 was introduced, **Public Safety Minister Vic Toews** announced that Bill C-30 would be sent to committee for review. As stated by **Minister Toews**, "***The government intends to send this legislation directly to committee for a full examination of potential amendments to update our laws while ensuring the privacy of Canadians is respected***," (*Edmonton Journal*, 2012-02-25, A12).

Criticisms / Concerns with Bill C-30

Warrantless Access to Subscriber Information

According to media, federal and provincial privacy commissioners are against police being able to obtain personal identifying data without a warrant. As stated by Assistant Privacy Commissioner Chantal Bernier, "The outstanding issue is warrantless access to personal information" (*Globe and Mail*, 2012-02-15, A6). North-West Territories Information and Privacy Commissioner Elaine Keenan-Bengts' stated that her largest concern with Bill C-30 is that it would give police and government the right to obtain personal information from internet users without a warrant or other means of judicial oversight. According to Keenan-Bengts, "Potentially, RCMP or other agents of the federal government, and those are not defined, will have access to everything you do, say or look at on the internet whether or not you are suspected of any wrong doing or criminal activity," (*Yellowknifer*, 2012-02-24). Similarly, Ann Cavoukian, Ontario's Privacy Commissioner, stated that Bill C-30 "will be the first, but steady, step of the creep of surveillance into the lives of law-abiding citizens," (*Calgary Sun*, 2012-02-15, 18).

Western Arctic MP Dennis Bevington expressed similar concerns, "I think the bill has come out and is very misguided. It's identified a problem that is not really a problem. I mean, police officers are capable of getting warrants to get personal information...This bill opens up the potential for abuse by authority and as such I'm very worried about it," (*Yellowknifer*, 2012-02-24).

The perceived potential for abuse was echoed by Lindsey Pinto, a spokesperson for OpenMedia.ca, "We're not seeing a very strong need for these bills, and we're seeing an expansion of surveillance powers that basically begs for abuse...We do need to make sure that there is clear oversight and really meaningful deterrence from abuse," (*Waterloo Region Record*, A10, 2012-02-21). A similar statement by Christopher Parsons, an online surveillance expert, stating that "It's absolutely critical – absolutely critical – that the legislation is clear," (*Edmonton Journal*, 2012-02-25, A12).

According to Michael Geist, an expert in Internet law at the University of Ottawa, Bill C-30 "creates a voluntary warrantless system that would allow police to ask for the content of emails or web surfing habits and allow ISPs to comply with the request without fear of liability," (*Vancouver Sun*, 2012-02-21, A3) and the bill will "fundamentally alter the Internet in Canada...It's in a sense Internet 2.0 and it's one that will embed surveillance capabilities throughout the network...[T]here really is no turning back once these surveillance capabilities are installed," (*Globe and Mail*, 2012-02-25, A5).

Privacy Concerns

Ann Cavoukian, Ontario's Privacy Commissioner, also stated that Bill C-30 could attract the attention of hackers looking to access the personal information of internet users. According to Cavoukian, "This is going to be like the Fort Knox of information that the hackers and the real bad guys will want to go after. This is going to be a gold mine... The government will say that they can protect the data, and they can encrypt it. Are you kidding me? The bad guys are always one step ahead," (*National Post*, 2012-02-15, A4).

Concerning privacy, online surveillance expert Christoper Parsons stated that "[t]his isn't just like picking up the phone book... It gives police the ability if you've been posting online to see where you've been posting, with what people and with what frequency. To suggest this is just 'phone book information' does a disservice to the public and is incredibly misleading," (*Vancouver Sun*, 2012-02-21)

Conservative MP John Williamson also expressed concerns with Bill C-30, stating, "I think it's too intrusive as it currently stands and does need to be looked at... There's a lot of concern I think across the country," (*Kingston Whig-Standard*, 2012-02-16, 11).

Bill C-30 and Locating Suspected Criminals

In June, **Public Safety Minister Vic Toews** stated that Bill C-30 would be helpful in apprehending criminal suspects who have gone on the lam, such as the high profile case of Luka Rocco Magnotta, stating, "***Certainly, that's what police have told me – that the powers in Bill C-30 are very relevant to this type of investigation in terms of either determining who the individual is, or determining the whereabouts of an individual***," (*London Free Press*, 2012-06-02, B3). These comments prompted criticism from the media (and public) alike (*Globe and Mail*, 2012-06-09, F2; *Globe and Mail*, 2012-06-09, F3; *Calgary Sun*, 2012-06-05, 15).

Support for Bill C-30

Support for Bill C-30

Media reported that Manitoba Justice Minister Andrew Swan expressed his support for Bill C-30, but would like to see amendments in regards to police requests for subscriber information from

Internet service providers. According to Swan, "Generally we've supported the idea behind Bill C-30...we agree with police that they need more powers to be able to go after hose individuals, at the same time we accept that Canadians have some real concerns about privacy," (*Winnipeg Sun*, 2012-04-24, 5).

The Ontario Association of Chiefs of Police expressed their public support for Bill C-30, stating that "We have supported the legislation because of a need by police to have crime prevention tools... We're dealing with legislation written in the 1970s, when rotary telephones were cutting-edge technology," (*Edmonton Journal*, 2012-02-26, A5).

The Winnipeg Police Service also expressed their support Bill C-30, stating that it will "provide police with the necessary tools to more effectively investigate serious crime" and will "modernize tools used by law enforcement and provide for the preservation of data and information," (*Winnipeg Free Press*, 2012-02-25, A4).

Charlottetown Police Chief Paul Smith also expressed his support for Bill C-30 (*The Guardian*, 2012-02-27, A1), along with Vancouver Police, the Canadian Police Association (*Toronto Star*, 2012-02-21, A7), Calgary Police (*Calgary Sun*, 2012-02-16, 22) and the Canadian Association of Chiefs of Police (*Winnipeg Free Press*, 2012-02-25, A4).

Broadcast Media

Broadcast media reported extensively on Bill C-30 during this period. Media coverage was concentrated in national media and was primarily negative in tone. The focus of this media coverage was on Minister Toews' comments during Question Period. The key concerns of critics of the legislation are the mandatory disclosure of subscriber information without a warrant and the privacy rights of Canadians. The main opponents of the legislation were interviewed several times during this period. They include Opposition party members such as MPs Charlie Angus, Jack Harris, Francis Scapaleggia and Dean Del Mastro. University of Ottawa professor Michael Geist was interviewed on three occasions about his opposition to the legislation.

CBC News and *CTV News* presented live coverage of a news conference by Minister of Public Safety Vic Toews, Minister of Justice Rob Nicholson and Senator Jean-Guy Dagenais to announce the Protecting Children from Internet Predators Act. (CBC News, CTV News, 12:45pm, 2012-02-14) CTV News Rough Transcript, CBC News Rough Transcript

CTV News presented live coverage of a news conference by NDP MPs Charlie Angus, Jasbir Sandhu, and Charmaine Borg on the Lawful Access bill. They disapprove of the bill because of privacy concerns and on the grounds that law abiding Canadians should not be treated as criminals. *RDI* a présenté un bref résumé de la conférence de presse. (CTV News, 10:30am; RDI, 14 :00pm, 2012-02-14) Rough transcript

CTV News interviewed Michael Geist regarding the Protecting Children from Internet Predators Act. The Minister was mentioned in this interview. He is concerned about the mandatory disclosure of subscriber information without a warrant. (CTV News, 16:10 ET, 2012-02-14) Rough transcript

CBC News Power & Politics interviewed MPs Charlie Angus and Francis Scapaleggia regarding the Protecting Children from Internet Predators Act. The Minister was mentioned several times in this interview. (CBC News, 17:00 ET, 2012-02-14) Rough transcript

RDI rapporte que le sénateur conservateur Jean-Guy Dagenais a affirmé que des vérifications ont été faites avec la Protectrice du citoyen du Canada et ses homologues provinciaux et que tous étaient d'accord avec la façon de procéder du projet de loi. (RDI, 6 :08am, 2012-02-15)

En entrevue avec le *98,5fm* pour l'émission *Dutrizac*, le sénateur conservateur Jean-Guy Dagenais affirme que l'intention première du projet de loi C-30 est de protéger les enfants des cyberprédateurs. La loi doit être modernisée pour s'harmoniser avec les nouvelles enquêtes policières. Le sénateur Dagenais affirme qu'avec le projet de loi, les policiers pourront retracer les gens mais ils ne regarderont pas le contenu de courriels. Dorénavant, les policiers n'auront pas besoin d'un mandat pour obtenir l'adresse IP d'un individu. (98,5fm, Montréal, 12:00pm, 2012-02-15)

CTV News Power Play interviewed MP Jack Harris regarding Bill C-30. (CTV News, 17:00 ET, 2012-02-15) Rough transcript

CTV News Power Play interviewed MPs Dean Del Mastro, Megan Leslie, and Robin Cuzner regarding the Conservative government being open to amendments to Bill C-30. (CTV News, 17:20 ET, 2012-02-15) Rough transcript

CBC News Power & Politics interviewed MPs Candice Hoeppner, Jack Harris, and Francis Scapaleggia regarding the Conservative government being open to amendments to Bill C-30. The interview included a quote from the Minister. (CBC News, 17:00 ET, 2012-02-15) Rough transcript

CBC News The National reported on reaction to the announcement of Bill C-30 and how personal information about the Minister has been revealed on Twitter. (CBC News, 21:07 ET, 2012-02-15) Rough transcript

CTV National News reported on backlash from Bill C-30. (CTV News, 22:05 ET, 2012-02-15) Rough transcript

En entrevue, Denis Barrette, avocat, porte-parole de la Ligue des droits et libertés explique que pour obtenir un mandat le policier aura à démontrer au juge qu'il a des motifs pour obtenir cette information car elle sera utile à son enquête. Selon lui c'est un abaissement des conditions pour l'obtention d'un mandat. Il dénonce le fait que la loi puisse être utilisée pour retracer des environnementalistes que le gouvernement fédéral a étiquetés comme terroriste. (RDI, 9:30am, 2012-02-16)

CTV News Power Play discussed the backlash from Bill C-30 with MPs Eve Adams, Jinny Simms, and Ted Hsu. Minister Toews was mentioned several times in this discussion. (CTV News, 17:25 ET, 2012-02-16) Rough transcript

CBC News Power & Politics interviewed Catherine Crump of the American Civil Liberties Union for insight on Bill C-30 and how similar laws have been applied in the U.S. The segment led off with a quote from the Minister on this topic. (CBC News, 18:45 ET, 2012-02-16) Rough transcript

CBC News Power & Politics interviewed cyber expert Jesse Hirsh for insight on the Twitter attack on the Minister and Bill C-30. (CBC News, 18:50 ET, 2012-02-17) Rough transcript

Global News' The West Block interviewed Waterloo Police Chief Matt Torigian and University of Ottawa professor Michael Geist on the Protecting Children from Internet Predators Act. (Global News, 11:00 ET, 2012-02-19) Rough transcript

CTV's Question Period interviewed MP's Dean Del Mastro, Jack Harris, and Marc Garneau on the Protecting Children from Internet Predators Act and social media response. (CTV News, 17:00 ET, 2012-02-19) Rough transcript

CTV's Question Period featured a panel discussion on Internet privacy and the backlash to the introduction of Bill C-30 featuring Colin Horgan with iPolitics, Lindsey Pinto with Open Media, and Alfred Hermida with UBC. (CTV News, 17:15 ET, 2012-02-19) Rough transcript

CTV News provided live coverage of Vancouver Police Department Deputy Chief Warren Lemcke's press conference regarding Bill C-30. (CTV News, 13:30 ET, 2012-02-20) Rough transcript

Broadcast media reported Minister Toews says he is surprised to learn that a section of bill C-30 provides for "exceptional circumstances" under which "any police officer" can request customer information from a telecommunications service provider. He admits that he has not read the entire bill. (98,5fm, Montréal, 12:00pm; RDI, 7:51am; CFRE-TV, Global Regina, 6:01am, 7:06am, 8:03am; CITV-TV, Global Edmonton, 6:12am; CFSK-TV, Global Saskatoon, 7:12am; CICT-TV, Global Calgary, 7:35am; SUN-TV, Toronto, 12:55pm; CFCF-TV, CTV Montreal, 12:33pm)

CBC News Power & Politics interviewed former Public Safety Minister Stockwell Day and NDP president Rebecca Blaikie regarding Bill C-30. (CBC News, 18:40 ET, 2012-02-21) Rough transcript

CBC News Power & Politics reported on the costs associated with Bill C-30, and spoke with MPs Pierre Polievre, Francis Scarpaleggia, and Jack Harris about these costs. (CBC News, 17:25 ET, 2012-02-22) Rough transcript

TV Ontario The Agenda interviewed OPP Commissioner Chris Lewis and Ontario Privacy Commissioner Ann Cavoukian regarding Bill C-30. (TV Ontario, 20:00 ET, 2012-02-22) Rough transcript

CBC News The National reported on the costs of Bill C-30. (CBC News, 21:05 ET, 2012-02-22) Rough transcript

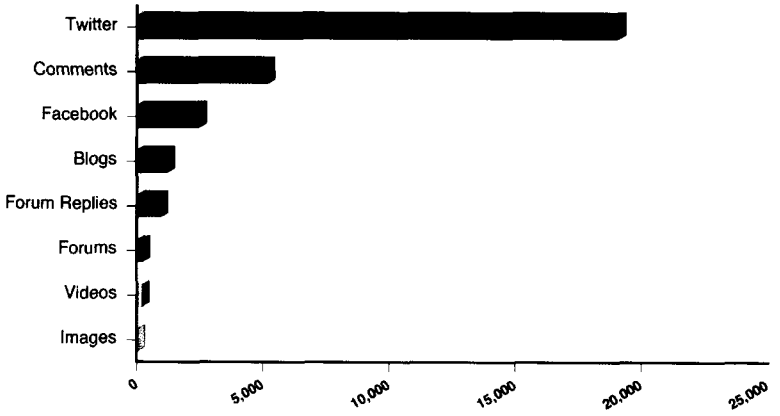
CTV News executive producer Barry Wilson was interviewed and gave a negative opinion of bill C-30 and of Minister Toews' handling of the issue. He describes the reaction to the bill as nothing short of remarkable and really a victory for true citizen democracy. (CFCF News, CTV Montreal, 12:30am, 2012-02-24)

CBC News Power & Politics reported on Bill C-30 and the case of Luka Rocco Magnotta and featured an interview with technology expert Michael Geist. (CBC News, 17:00 ET, 2012-07-11) Rough transcript

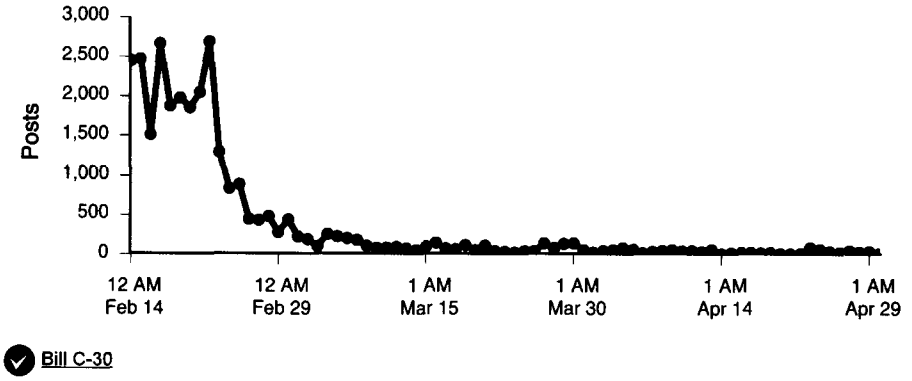
Social Media Overview

February – April

The bulk of the activity occurred in the first segment, when Bill C-30 was mentioned approximately 30,000 times, distributed across social media platforms as follows:



During this period, activity spiked three times on February 15, 17 and 22.



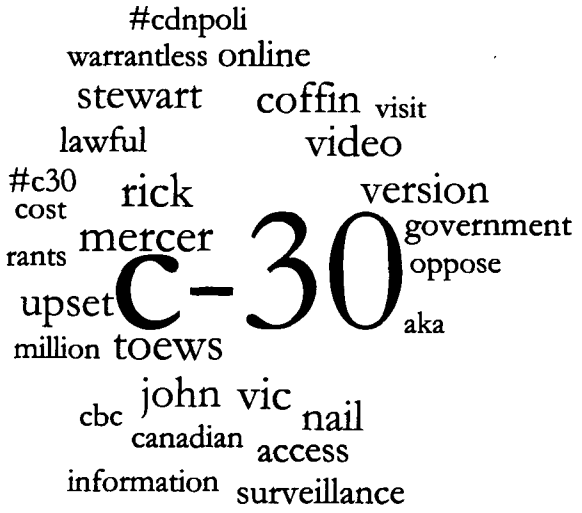
Spike 1: An opinion piece from the Toronto Star was shared broadly.

Example tweet:

Capital Squirrel: "Conservative Bill C-30 will let police spy on Canadians online" http://t.co/3IIGFq33 #cdnpoli #privacy #CPC #BillC30 #Internet

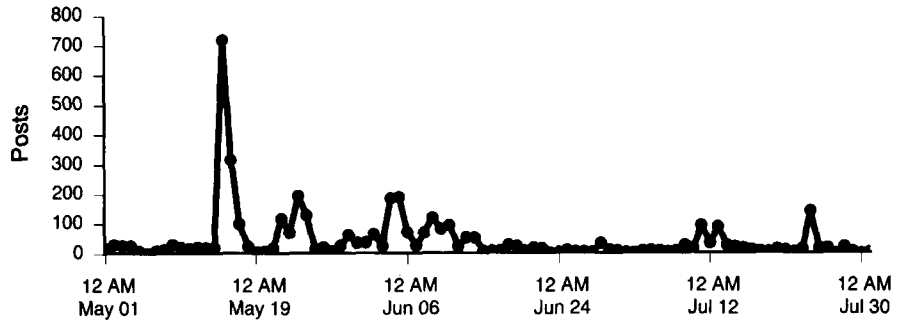
Spike 2: Discussions about the #TellVicEverything hashtag on online forum Slashdot.

Spike 3: The sharing and discussion surrounding a YouTube video by Rick Mercer.



May – July

The bulk of social media activity mentioning Bill C-30 in this segment involved the sharing of a tweet by Justin Trudeau on May 15:



justinpjtrudeau: #TellVicEverything was a smashing success: Bill C-30 is gone. See, these guys can be stopped if we all stand together. http://t.co/9hkBIIt3

August

The bulk of social media activity mentioning Bill C-30 in August involved tweeting about the IFLA World Library and Information Congress.

Example tweets:

ingalunden: Surveillance as necessary for your safety. Who defines my safety? (Un)lawful access Jeannie Bail Canada #WLIC2012 pic.twitter.com/UQONOxxM

libswell: #wlic2012 Bill C-30 is overly intrusive, too light oversight by courts, expensive, potential for privacy breaches #FAIFE

Alex Byrne: #wlic2012 privacy commissioner in Canada has helped block lawful access legislation to date #FAIFE

Surveys / Petition

Two surveys were conducted regarding Bill C-30; one by Angus Reid released on February 24, 2012 and another by Ipsos Reid released on February 29, 2012.

OpenMedia.ca started an online petition to stop Bill C-30 from going forward. To date, the petition has been signed by over 145,000 people.

Public Safety Activity

Between February 14, 2012 and August 28, 2012 Public Safety Canada received 16 related media calls as well as 27 public enquiries.

Key quotes

"The outstanding issue is warrantless access to personal information." - **Assistant Privacy Commissioner Chantal Bernier** (The Globe and Mail, A6, 2012-02-15)

"This will be the first, but steady, step of the creep of surveillance into the lives of law-abiding citizens." - **Ann Cavoukian, Ontario's privacy commissioner** (Calgary Sun, 18, 2012-02-15)

"The police have been using our system of warrants and judicial authorization for many years with great success ... the system is working, and the beauty of it is it goes after the bad guys." - **Ann Cavoukian, Ontario's privacy commissioner** (National Post, A4, 2012-02-15)

"Now, every single Canadian citizen is walking around with an electronic prisoner's bracelet. I say to Vic Toews, Stop hiding behind the boogey man. Stop using the boogey man to attack the basic rights of Canadian citizens.' Is Vic Toews saying that Stockwell Day supports child pornography? Is Vic Toews saying that every privacy commissioner in this country who has raised concerns about this government's attempt to erase the basic obligation to get a judicial warrant, is he saying that they're for child pornography?" - **NDP MP Charlie Angus** (National Post, 2012-02-14, 15:29 ET)

'We've been really challenged with criminals committing old crimes with new technology and we're really handicapped in our ability to get into these new technologies." - **Calgary police Deputy Chief Murray Stooke** (CBC News)

'I think our police have a lot of tools and they know how to use them. This bill takes it completely out of balance putting the onus on everybody, that all of our surfing history should be preserved and that's just not a good thing." - **Tom Keenan, professor at the University of Calgary, internet security expert** (CBC News, 2012-02-15)

"On travaille encore avec des lois qui ont été écrites à l'époque du téléphone à cadran." - **Francis Brabant, conseiller juridique à la Sûreté du Québec et porte-parole de l'Association canadienne des chefs de police** (La Presse, A14)

"It's the kind of privacy protection that courts who have looked at this issue in any number of different cases, not just in crime cases, but also dealing with copyright and the like, have said that's how we try to strike a balance. And what the government is doing with this legislation is throwing that balance out entirely. Saying that there can be mandated disclosure, no court orders" - **Michael Geist, a professor at the University of Ottawa and expert on cyberlaw** (CTV News, 4:10pm, 2012-02-14)

"The government has yet to provide detailed information about the cost of the technical infrastructure ISPs must install. Nor is it clear just how sparingly police officers will use the warrantless information request powers. But some of the proposed uses of the bill, such as alerting someone when their stolen property has been recovered, don't fit that framing." - **Michael**

Geist, a professor at the University of Ottawa and expert on cyberlaw (The Globe and Mail, A6, 2012-02-15)

"There are philosophical, privacy, and practical issues to this that have been pointed out to the government but they've decided to proceed ahead anyway, If this is brought in, for sure there will be constitutional challenges to it. The argument from those opposed is going to be it's unreasonable search and seizure of their personal information without any judicial authority. That has a reasonable good chance of succeeding." - **Mark Hayes, partner with Hayes eLaw LLP in Toronto** (Canadian Lawyer & Law Times blog, 2012-02-14)

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Willey, Chris

From: Therien, Stephane on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: Wednesday, February 15, 2012 11:55 AM
To: * COMMS ADG / Bureau du directeur géneral associé; * COMMS Communication Services Division / Division des services de communication; * COMMS DGO / Bureau de la directrice générale; * COMMS Program Communications Division / Secteur des communications de programmes; * COMMS Public Affairs Division / Secteur des affaires publiques; * Speeches / Discours; Astravas, Rutha; Banerjee, Ritu; Beaudoin, Serge C; Bolton, Stephen; Boucher, Patrick; Boucher-Lalonde, Murielle; Cameron, Bud; Carmichael, Julie; Champoux, Elizabeth; Clairmont, Lynda; Coburn, Stacey; Crawford, Andrée; Csversko, Christine; Currie, St. Clair; Daoust, Normand; De Santis, Heather; Duschner, Gabrielle; Dussault, Josée; Easson, Grant; Gareau-Lavoie, Genevieve; Gordon, Robert; Hitchcock, Christy; House, Andrew; Huggins, Rachel; Humeniuk, Elena; Hunt, Ryan; Jarmyn, Tom; Johnson, Mark; Kelland, Stephen; Khouri, Lisa; Komm, Chantelle; Kubicek, Brett; Lavoie, Micheline; Leclair, Natalie; Leclerc, Carole; Leonidis, Nelly; Lesser, Robert; MacDonald, Nicholas; MacKinnon, Paul; Marchand, Renee; McAteer, Julie; Morris, Marika; Motzney, Barbara; Mundie, Robert; Nicole, Jean-Thomas; Oldham, Craig; Panthaky, Jasmine; Patton, Michael; Pozhke, Nicholas; Rosario, Giselle; Roy, Isabelle; Saunders, Joanne; Shuttle, Paul; Slack, Jessica; Thibault, Stéphane; Tupper, Shawn; Van Criekingen, Jane; Verret, Scott; Wex, Richard; Wilson, Gina; Adam.Kates@cbsa-asfc.gc.ca; Allison.Wildgust@cbsa-asfc.gc.ca; Amitha.Carnadin@cbsa-asfc.gc.ca; Bateman, Paul; Bernard.Alladin@cbsa-asfc.gc.ca; Bindman, Stephen; Brunette, Lynn; cbsa.media@cbsa-asfc.gc.ca; Cgirouad@justice.gc.ca; Chad.Fleck@international.gc.ca; Williams, Christpher; Churney, Daryl; Cocking, Marie; Couture, Jocelyne; Derek Cefaloni; Douglas, Caroline; Van Allen, Elizabeth; C. Girouard; Bradley, Jolene; Mackillop, Ken; Lamothe, Maureen; Lauzon, Raymond; Lavoie, Daniel; MacDonald, Jane; Mailhot, Esther; Stokes, Mark; Mary.Schlosser@rcmp-grc.gc.ca; RCMP Media Monitoring; Melissa Hart; Martin, Nadie; Robinson, N.; Giolti, Patrizia; Prieur, Mark; Rioux, Veronique; Rondeau, Martine; Sbinman@justice.gc.ca; Dumoulin, Stéphanie; Tim.Cogan@rcmp-grc.gc.ca
Subject: Media Snapshot: Protecting Children from Internet Predators Act / Loi sur la protection des enfants contre les cyberprédateurs, 15-02-2012

Protecting Children from Internet Predators Act / Loi sur la protection des enfants contre les cyberprédateurs
Media Snapshot | Aperçu médiatique

15-02-2012

Key issues and overview

- This issue has received a significant amount of national and regional media attention from all media types. The vast majority of the media attention has been highly negative in tone primarily focusing on the comment Minister Toews made in the House of Commons on February 13 regarding child pornography and on privacy concerns. A significant number of negative comments have been published on the subject.

Key quotes

"The point here is this can no longer be discretionary on the part of telecommunication service providers, especially when children's lives are at stake. It's clear we need a better system." - **Public Safety Minister Vic Toews** (Ottawa Citizen, A3)

"There is nothing in the bill that would allow police to snoop on an individual's private conversations or even to follow a person's activities on the Web. All that has to be done through a judicially authorized warrant." - **Public Safety Minister Vic Toews** (The Globe and Mail, A6)

"The outstanding issue is warrantless access to personal information." - **Assistant Privacy Commissioner Chantal Bernier** (The Globe and Mail, A6)

"This will be the first, but steady, step of the creep of surveillance into the lives of law-abiding citizens." - **Ann Cavoukian, Ontario's privacy commissioner** (Calgary Sun, 18)

"The police have been using our system of warrants and judicial authorization for many years with great success ... the system is working, and the beauty of it is it goes after the bad guys." - **Ann Cavoukian, Ontario's privacy commissioner** (National Post, A4)

"We've been really challenged with criminals committing old crimes with new technology and we're really handicapped in our ability to get into these new technologies." - **Calgary police Deputy Chief Murray Stooke** (CBC News)

"I think our police have a lot of tools and they know how to use them. This bill takes it completely out of balance putting the onus on everybody, that all of our surfing history should be preserved and that's just not a good thing." - **Tom Keenan, professor at the University of Calgary, internet security expert** (CBC News)

"On travaille encore avec des lois qui ont été écrites à l'époque du téléphone à cadran." - **Francis Brabant, conseiller juridique à la Sûreté du Québec et porte-parole de l'Association canadienne des chefs de police** (La Presse, A14)

Print Media

The tabling of the *Protecting Children from Internet Predators Act* in the House of Commons received extensive national and regional print media coverage. The tone of coverage was negative and focused on the transfer of customer information to police without a court order as well as reactions to comments by Minister Toews from the previous day. A large number of negative editorials and opinion pieces were published on the subject.

Online surveillance bill gets rough ride in House
Prime Minister Stephen Harper called on parliamentarians Tuesday to stand firm against child pornography and support a contentious bill that will require telecommunications companies to hand over customer information to police without a court order. But opposition parties hit back hard by predicting the new bill will lead to an infringement of the privacy of Canadians, saying it will allow police to build a detailed profile of people, including law abiding citizens, using their digital footprint - without any judicial oversight. They also blasted one of Harper's **senior ministers** who told a critic of the bill he "can either stand with us or with the child pornographers." **Public Safety Minister Vic Toews** inflamed matters Monday by saying that an opponent of the bill "***can either stand with us or with the child pornographers***." This comment dominated question period, with opposition parties calling on Harper to explain them. **Toews**, when pressed by reporters Tuesday, said that to characterize an opponent of the legislation as standing with child pornographers "is not a fair comment," claiming he never made such comments in the House of Commons Monday. Currently, telecom companies can provide the personal information of customers on a voluntary basis. Companies turn over the information to law enforcement agencies in about 95 per cent of cases, but the turnaround time takes an average of 13 days, **Toews** told reporters Tuesday. "***The point here is this can no longer be discretionary on the part of telecommunication service providers, especially when children's lives are at stake. It's clear we need a better system***," said **Toews**. Ottawa Citizen, A3 (Leader-Post, Starphoenix, Edmonton Journal, Calgary Herald, The Province, Montreal Gazette, New Brunswick Telegraph-Journal, Times & Transcript, Times Colonist); National Post; Calgary Sun (Edmonton Sun, Ottawa Sun, Kingston Whig-Standard, Windsor Star, London Free Press); Waterloo Region Record (Chronicle-Herald, The Guardian, Red Deer Advocate, The Telegram, Whitehorse Star); Le Devoir; La Presse (La Tribune, Le Droit); Globe and Mail; Le Quotidien; Journal de Montréal

Surveillance bill grants police access
The Conservative government's new and controversial online surveillance bill will likely have wide-ranging consequences for the way the Web works in Canada - even if many of these consequences are still difficult to foresee. Dubbed the Protecting Children from Internet Predators Act, the proposed law gives police departments the ability to obtain personal information about Canadian Internet users without a warrant. Globe and Mail, A6; Le Soleil

Toews returns to divisive scare tactics
An opinion piece states, "**Public Safety Minister Vic Toews'** attempt to demonize opponents of his new Internet law - you're either with the government, or with the "***child pornographers***," he said on Monday - isn't the first time he's sought to demonize critics. In November, he said Liberals should "***finally stop putting the rights of child pornographers and organized crime ahead of the rights of law-abiding citizens.***" Two weeks ago, he urged the NDP "***to listen to the police, listen to the provinces, and support these balanced measures that protect law-abiding Canadians and their children.***"...But the facts don't support any of the **Minister's** statements...Even bureaucrats in **Mr. Toews'** own

department aren't buying his arguments...**The Minister** has tried to set this up as a left/right issue, but it transcends the political spectrum. It's in everybody's interest not to have the government monitoring their every online move, especially at a time when more and more of our daily lives are being conducted over the Internet...This is all part of a much larger campaign, conducted by the Harper government, that has served only to alienate many Canadians...Mr. Harper launched a scathing attack on libertarians, who he - using twisted logic that almost rivals that of **Mr. Toews** - basically accused of causing the financial collapse...When **Public Safety Minister Vic Toews** defended his "lawful access" legislation by saying that people "***can either stand with us or with the child pornographers,***" he made the issue pretty black & white. Steve Murray wonders what other issues are as stark in **Toews's** mind." National Post, A4

Crime fixation bizarre in face of Tories' common sense
An opinion piece states, "Bob Rae can gripe about "evidence-based decision-making" all he likes. The truth is that, on the big economic files, Conservatives are the party most consistently hewing to reason and common sense. It's why they keep getting elected. All of which makes their bizarrely irrational, ham-fisted, counterproductive handling of justice and security all the more odd. What do Rob Nicholson and **Vic Toews** think they're achieving, beyond throwing occasional hunks of dripping meat to a social conservative base that, truth be told, is secure without it? Are they afraid the Charles Bronsons across the aisle will accuse them of being soft on crime? Here's a thought: Perhaps Tories should rather begin to worry that fair-minded Canadians from all regions may come to view them as demagogues...First, prison farms: not a kitchen table issue for most voters, admittedly...There was the Tackling Violent Crime Act - its centre piece, mandatory minimums for people convicted of "serious gun crimes."...There's Bill C-10 itself - a grab-bag of nine pieces of legislation the Tories tried but failed to land pre-majority...It bears repeating: Rates of violent crime have fallen steadily since the early 1990s...But all that has been a mere preamble to two astonishing recent forays **by Public Safety Minister Toews**. First it emerged that in 2010 he told the Canadian Security Intelligence Service that where human life is at risk, Canadian spies can use information obtained by torture - overturning years of Canadian policy, including Conservative policy, and the findings of the 2005 Arar Inquiry. No answer yet, to this question: When, where the security agencies are involved, is human life not at risk? Then this week, not to be outdone by himself, **Toews** blurted that opposition critics of his new online surveillance bill, tabled Tuesday - which gives police unprecedented power to obtain private data without a warrant - are siding with "child pornographers."...**Toews** should give his head a shake. If he can't or won't, the prime minister should." Ottawa Citizen, A3 (Starphoenix, Leader-Post, Montreal Gazette, Edmonton Journal, Calgary Herald, Vancouver Sun, The Province)

Vic Toews goes phishing
An editorial states, "The Harper government has curious views of individual freedom and privacy. On the one hand, the federal Tories wrongly decry the long-form census as an invasion of privacy and correctly declare the long-gun registry as a heavy-handed government intrusion into the lives of law-abiding citizens. Yet those who dare raise privacy concerns about the government's proposed online-surveillance legislation are accused of supporting pedophiles and child pornographers. This absurd, insulting and offensive suggestion, uttered Monday by **Public Safety Minister Vic Toews**, demonstrates a philosophy of convenience on the part of the Harper Tories...On Monday, when Liberal MP Francis Scarpaleggia pointed out the privacy concerns surrounding the government's lawful access legislation for electronic surveillance, **Toews** responded, "**He can either stand with us or with the child pornographers." It was a classic "fer us or agin us**" moment, ranking right up there with the utterance by George W. Bush, that, "Either you are with us, or you are with the terrorists," which rendered any opposition to the war in Iraq as unpatriotic. This is not the first time the government has outrageously accused its tough-on-crime opponents of favouring pedophilia...It was ironic that **Toews'** remark came the same day that a judge rightfully declared as unconstitutional the mandatory three-year minimum for a gun crime, which was a key Tory initiative...If the police have reasonable grounds for illegal online activity, they can get a warrant, not go on phishing expeditions by snooping in the computers of ordinary Canadians." Calgary Herald, A14

With 'em or against 'em
An editorial states, "The Conservatives have their majority. They no longer have any excuse to act like schoolyard bullies. Yet they can't seem to stop. **Public Safety Minister Vic Toews** has been the worst offender lately, demonizing anyone who dares criticize his policy. When the Opposition raised valid questions about the government's quiet directive to use information obtained by torture, **Toews** responded, "***The NDP would not take appropriate action to ensure that the lives of Canadians were protected***" in an emergency. "***That is why those members are over there. They are not fit to be trusted with the security of Canadians***." As a veteran politician who spent six years on the other side of the House himself, **Toews** should be wary of ad hominem attacks based on a party's electoral fortunes. They could very well come back to haunt him. This week, **Toews** moved on to legislation that will allow the state easier access to the private information of Canadians - the Protecting Children from Internet Predators Act. In response to a question from Liberal Francis Scarpaleggia about why Canadians should trust the government to only use these powers for their stated purpose, **Toews** went on the offensive again, saying Scarpaleggia "***can either stand with us or with the child pornographers***."...If **Toews** is sure of his ground, he could have simply articulated his arguments and let them stand on their merits. His choice to reduce the debate to insults suggests that the government's policies on torture and Internet snooping are not as unassailable as the Conservatives pretend..." Ottawa Citizen, A14

The Tories weren't elected to spy on us
An editorial states, "Three days before the May 2 federal election when Stephen Harper and his Tories won a majority, this news-paper endorsed him and his party to govern Canada. We did that for two reasons: a belief, after too many years of ineffective minority governments, that Harper was the only leader capable of forming a majority, and a view that the Harper team would best manage Canada's economy and federal spending. Many Canadian voters agreed. But we now join what should become an even larger (and hopefully louder) majority of Canadians in denouncing and opposing the Tories' so-called "lawful-access" legislation that will give police unprecedented access to the personal information of Internet users - names, addresses, phone numbers and online ID numbers - without court oversight. We are also disgusted - a strong word, but accurate - at **Public Safety Minister Vic Toews's** statement that those who oppose his police-state laws are supporters of pedophiles and child-pornographers. That's an appalling thing for **Toews** to say about his fellow Canadians and he should apologize..." The Province, A20

Scrutiny yields stronger laws
An editorial states, "The speed with which digital technology has changed the world of communication has created unprecedented opportunities for innovators and criminals alike. In that light, it is imperative that Canada modernize its laws that regulate the telecommunications industry, protect users and make innovation more inviting...Since governments have been trying for years to modernize Canada's laws related to the Internet and digital communications devices, you'd think that the ministers involved would have done more to get the critics on-side. Instead, **Public Safety Minister Vic Toews** kicked off the debate by suggesting that anyone who questioned the government's ability to draft a proper bill would rather support child pornographers than the forces of good...In announcing the legislation, **Mr. Toews** made it clear that some companies already provide information, others do it on a case-by-case basis, and some refuse. The legislation will provide some uniformity across the industry, which makes things fairer since it costs the service provider money to comply. **The minister** also credibly argues that police need this information to apply for a court order they are required to have in order to read or monitor anything on the equipment. Privacy officials insist, however, that a court order should be issued in advance of divulging any personal information...Using simple-minded names for important bills, and using simple-minded insults to defend them, does a disservice to Canadians and makes it more difficult to enact balanced legislation..." Starphoenix, A8

New bills encroach on our privacy
An opinion piece states, "...In its own determined haste to rewrite the current Criminal Code, the Conservative government would rather push us in the direction of 1984. George Orwell's Nineteen Eighty-Four, that is...However, the government on Tuesday tabled bills C-50 and C-51, its ironically named "lawful access" legislation. Today, it is nothing of the sort. Our current government believes it should have the right to invade not only our bedrooms but our telephone conversations and computer hard drives - surreptitiously and without regard for accepted judicial process - on the supposition that the guilty will be more easily unearthed if the innocent also have to surrender their expectation of privacy to faceless investigators. It is as if Conservatives like Harper and **Public Safety Minister Vic Toews** see value in having the powers of Big Brother. **Toews** recently defended the proposed legislation against a pointed attack by saying you either support the bills or you support child pornographers, and in so doing he defaulted to the lowest common denominator. In a majority House, that apparently passes for debate. In a free world, however, this legislation does not pass the smell test..." Edmonton Journal, A22

Big Brother has no place in our computers
A letter to the editor states, "In responding to Liberal criticism of a bill that would give law enforcement new powers to access Canadians' electronic communications, **Vic Toews** has been quoted as saying: "***He can either stand with us or with the child pornographers***." I spent 23 years in the military, have most likely had my Department of Veteran Affairs file passed around inappropriately just as other veterans have experienced, and our **Public Safety Minister** has the nerve to say this about me and other Canadians? Yet, I oppose any legislation that would put "law-abiding citizens" under the umbrella that **Mr. Toews** has opened up over all Canadians. I demand an apology in the House for his stupidity and arrogance and for making all Canadians who oppose this bill out to be child pornographer supporters..." National Post, A11; National Post

T'as des choses à cacher ?
Un article d'opinion déclare, « Ainsi, selon **le ministre fédéral de la Sécurité publique Vic Toews**, si vous n'appuyez pas le projet de loi conservateur sur la surveillance électronique (qui permettra aux policiers et aux services de renseignement d'avoir accès plus facilement à des informations confidentielles sur les internautes -- vos codes, vos coordonnées, les sites que vous consultez), c'est que vous êtes du côté des pédophiles... » Journal de Montréal, 6

Tories' terrifying online surveillance bill
An opinion piece states, "One can only congratulate **Canada's Public Safety Minister Vic Toews** for taking George W. Bush's Churchillian call to freedom in 2001 - "you're either with us or with the terrorists" - and raising him one with

Monday's House of Commons classic, "***He can either stand with us or with the child pornographers.***" **Toews** was speaking of a conscientious Liberal MP who had dared question the Harper government's new bill allowing free-ranging police online surveillance of Canadians. Francis Scarpaleggia, the Liberal public safety critic, had been doing his job - rather well, in fact - by saying that the bill has police "preparing to read Canadians' emails and track their movements through cellphone signals, in both cases without a warrant." The lovely and fragrant **Toews**, a towering intellect and rollerblader - I'm only saying this in preparation for my arrest on child porn charges, when I'll require traction for my abject begging - guards our children with a Tea Party level of threat and thuggery...So **Toews** got carried away. Or did he? The Conservatives are punitive and paranoid. What's so private that you wouldn't want the RCMP to see it? Something to hide, buddy?...A smart journalist wouldn't be writing this column, the very existence of which must lead **Toews** to conclude that I not only enjoy but probably manufacture child porn in my off-hours to the point that I have already applied for a daycare licence...But the Conservatives claimed to hate the registry because it invaded the privacy of law-abiding people. They were lying. This government hates privacy..." Toronto Star, A23

Welcome to Big Brother government
An editorial states, "In Ottawa, we have a federal government that this week will finally dismantle the federal long-gun registry. It will do this because it believes that forcing law-abiding gun owners to tell the government what kinds of guns they have is an affront to privacy and liberty. To supporters of the Conservative government -- and to the government itself -- the long-gun registry was a a symbol of all that is wrong with so-called Big Brother government... And yet, on Tuesday, this very same government tabled new legislation which would give police, spies and federal bureaucrats from the Competition Bureau the power to collect information about the digital services Canadians use without first obtaining a warrant from a judge. There is no excuse for this kind of intrusion on the privacy rights of Canadians and certainly not one from a government that says it champions the idea that the federal government ought to respect individual liberties and rights...**Toews** would have you believe that the NDP, civil rights advocates, privacy commissioners and other opponents of this draconian legislation support child pornographers, the bill's alleged target. Baloney... All **Toews** has done is cave to pressure from a law enforcement lobby to create a shortcut that does away with important judicial oversight of the investigators. That's about as Big as Big Government gets..." Edmonton Sun, 15 (Calgary Sun, Ottawa Sun, London Free Press)

Good questions deserve answers
An editorial states, "**Vic Toews, Canada's Public Safety Minister**, has drawn the battle lines in the debate over the policing of cyberspace in the following way: There will be those who stand with the government's Protecting Children From Internet Predators Act, and those who stand "with the child pornographers." The best word to describe the **minister's** utterance is "silly." It is unworthy of our Parliament and stands no chance of intimidating critics of the new bill, which was tabled on Tuesday...These are good questions, **Mr. Toews**. When it comes to balancing criminal law with the rights of individuals, anyone who does so in good faith is standing with the angels." Globe and Mail, A16

A worrying foray into our private communications
An editorial states, "**Federal Public Safety Minister Vic Toews** has tarred anyone opposed to the federal government's impending "lawful-access" legislation as someone who favours the rights of child pornographers and organized crime ahead of those of lawabiding citizens...In making the argument for abolition of the long-gun registry, **Toews** and others in the government charged that the registry treats law-abiding gun owners like criminals. Yet with this legislation, the same government would allow police to treat all Canadians like criminals, with or without evidence to that end." Montreal Gazette, A18

ONLINE SURVEILLANCE BILL
A letter to the editor states, "So **Toews** pulls out the argument that anyone who doesn't like the idea of the government spying on them is siding with child pornographers. This is a strange position for a government to take that has, in the last couple of years, through the CRTC, given licences to two porno channels to operate in Canada...This is using an illogical emotional argument to override both the Magna Carta, what's left of it in Canada, along with the constitutional protection in Section 8 of the Charter against unreasonable search and seize. Leave the children out of it, **Mr. Toews**, and get a warrant." Ottawa Sun, 14

Débat primaire sur Internet
Un article d'opinion déclare, « Les ministres de la Justice sont habituellement des politiciens effacés et **Vic Toews** ne cadrait pas tout à fait dans le moule. Le premier ministre Stephen Harper l'a rapidement muté après moins d'un an en poste. Aujourd'hui responsable de la **Sécurité publique** pour le gouvernement conservateur, il n'a pas modéré ses transports...Il ne faut pas se laisser berner par le nom accrocheur : l'intention ministérielle a bien peu à voir avec la protection des enfants qui pourraient être la cible d'abuseurs qui se servent d'Internet pour harponner leurs jeunes victimes, même si ça peut aussi servir à ça. Le problème, c'est que les spécialistes des questions de crimes contre les mineurs, ceux qui militent pour la protection des libertés civiles et ceux, enfin, qui s'intéressent aux questions relatives à la protection de la vie privée ont tous soulevé des hésitations...Le **ministre Toews** utilise le langage provocateur qu'il

emploie depuis des années comme ministre, à Ottawa depuis 2006 comme au Manitoba, entre 1995 et 1999. L'homme n'a foncièrement pas changé et son obsession avec la loi et l'ordre n'en démord pas. Il utilise aussi un vieux truc, soit d'associer un projet de loi avec une cible bien précise les cyberprédateurs et avec une cible bien précise, les enfants. Mais le texte suggéré peut être interprété de manière bien plus large que simplement doter la police d'outils essentiels pour lutter contre un affreux crime...Non seulement le gouvernement n'a pas expliqué comment les présents pouvoirs de la police doivent être élargis, le **ministre Toews** a gaffé en plaçant tous ceux qui questionnaient son projet de loi C-30 dans le camp des cyberprédateurs. Le **ministre** utilise une tactique simpliste, binaire, que les conservateurs utilisent régulièrement. George W. Bush l'a fait de façon répétitive pendant ses deux mandats à la présidence des États-Unis. « Ou bien vous êtes avec nous, ou bien vous êtes contre nous. »...Aujourd'hui, 80 % des Canadiens utilisent Internet de façon régulière...Ils devraient être tout aussi suspicieux de l'intention du gouvernement dans les pouvoirs qu'il veut se doter quant à leur identité sur Internet. Mais se feront-ils accuser d'être des alliés des pornographes et autres prédateurs sexuels ? **Vic Toews** limitera-t-il leurs objections à cela ? » Le Droit, 18

Big Brother has no place in our computers
A letter to the editor states, "The National Post editorial board woke up one day and discovered that this Tory government has autocratic tendencies. That they're really big on some freedoms - like the right to anonymously keep a Ruger Mini in your home - but not too big on others..." National Post, A11

Online Media

Online media coverage was extensive and negative in tone. Coverage focused on the new legislation that would make it easier for law enforcement to conduct electronic surveillance. The official Opposition and stakeholders stated there is no justification for the legislation citing privacy concerns.

Minister says Canada needs online surveillance law to chase cyber-criminals
Justice Minister Rob Nicholson says new legislation will give police and security services the tools they need to deal with sophisticated cyber-criminals. The legislation introduced today would allow authorities access to Internet subscriber information -- including name, address, and email address -- without needing a warrant . . . But **Public Safety Minister Vic Toews** says that unless the bill is adopted, it will allow child pornographers and organized crime to flourish. iNews880; Shanghai Daily; CIO

Online surveillance bill goes too far: Calgary professor
A Calgary internet security expert says Ottawa's new online surveillance bill violates the privacy of many to catch a few. The bill gives police and intelligence agencies new powers to access people's electronic communications without a warrant. CBC News; iPolitics; News Talk 650 CKOM; 680 News; RT

Community reaction to controversial online surveillance bill
A bill that would give police and intelligence agencies unprecedented powers to access Canadians' electronic communications and personal data, without a warrant, has sparked a firestorm of controversy. The proposed Protecting Children from Internet Predators Act was tabled in the House of Commons Tuesday. It would require internet service providers and telecommunications companies to share customer information with authorities when requested, without court oversight. **Public Safety Minister Vic Toews** says the legislation is needed to take down child pornography rings and organized crime in the 21st century. CBC News

Canada creeping toward Big Brother state with online surveillance bill, critics warn
An online surveillance bill tabled Tuesday in Canada gives law enforcement 21st-century tools, and those who don't support it side with child pornographers, the public safety minister said. The ruling Conservative government introduced the legislation as expected a day after **Public Safety Minister Vic Toews** derided the opposition for criticizing the bill. Global Post; Examiner

'Snoop and spy' bill could be costly overreach
An opinion piece states, "**Vic Toews, Canada's Public Safety Minister**, has framed any debate of the Conservative government's new lawful access bill in the simplest terms: Canadians can either stand with the government, or with child pornographers..." Globe and Mail

The House of Commons is getting strange... really strange
An opinion piece states, "Does **Vic Toews** have amnesia? Or is he just plain crazy? Toews, who is Canada's Public Safety Minister, has been generating a lot of online buzz these past few days. During a debate this week about internet privacy, Vic Toews called those who disagree with the new Tory bill child pornography sympathizers..." CJAD

Say hello to Big Brother Government
An opinion piece states, "**Toews** would have you believe that the NDP, civil rights advocates, privacy commissioners and other opponents of this draconian legislation support child pornographers, the bill's alleged target. Baloney. The bill lets bureaucrats from the Competition Bureau get personal details without a warrant. The Competition Bureau is now tracking down kiddie porn perverts?..." Sun News Network

Bill aimed at internet predators empowers Big Brother government
An opinion piece states, "...This debate is not a matter of standing with the government or the child pornographers, as **Canada's Public Safety minister Vic Toews** disgracefully suggested to his fellow parliamentarians. If it was, then all of Canada's privacy commissioners would be standing with the child pornographers, as the NDP's Charlie Angus pointed out..." iPolitics

Gov't Internet surveillance bill goes too far
An opinion piece states, "We're all for law and order in Canada, but **Public Safety Minister Vic Toews'** comment that accompanied Tuesday's introduction of the online surveillance bill is an insult to the vast majority of law-abiding citizens of this country..." Medicine Hat News

Canada: The new cyber snoop state
An opinion piece states, "The Canadian Conservative government always depicts itself as on the moral high ground when it comes to legislation on crime. The new bill has the grandiose title: Protecting children from internet predators act. Only in the title are children and predators mentioned. In fact according to the CBC article the title appears to have been changed when the bill was sent to the printers..." All Voices

Stockwell Day warned Tories against internet snooping
An opinion piece states, "Team Harper should have listened to Stockwell Day. When Day was Public Safety minister, he opposed the type of digital snooping that his successor, **Vic Toews**, is bringing forth with Bill C-30..." iPolitics

Broadcast Media

Broadcast media attention was moderate and has decreased from the previous day. Reports focused privacy concerns and on Minister Toews' comments.

Broadcast media reported opposition parties and civil liberties advocates are reacting with outrage to a bill that would give police sweeping powers to monitor Canadian cell phone and internet use without a warrant. (CBO-FM, Ottawa, 6:30am, 7:34am; CFRE-TV, Regina, 6:16am; CFCN-TV, CTV Calgary, 6:57am; CIII-TV, Global Toronto, 6:27am)

CTV Morning Live reported **Minister Toews** stated in the House of Commons that the bill includes limitations on what police have access to. (CTV Morning Live, CHRO-TV, Ottawa, 6:32am, 8:02am)

CHCH News reported **Minister Toews** is rejecting criticism of a new bill that would allow police to obtain personal information without a warrant. (CHCH News, Hamilton, 7:30am)

Ottawa Morning interviewed **Minister Toews**. He explained that the bill, as in other countries, allows the police to obtain from an Internet service provider certain identifiers, a name, e-mail, telephone book information. That information is then used in the course of a criminal investigation in order to get a warrant. He stated that before police are allowed any access to the substance of a persons e-mail or web surfing history, there has to be judicial authorization. He added the bill puts forth a legal framework that not only allows the police, in appropriate circumstances, to ask for an IP address but then demands accountability of the police because an annual report is compiled, provided to the attorneys general in every province for them to review, as well as the Privacy Commissioner. (CBC Radio One, Ottawa Morning, 7:46am)

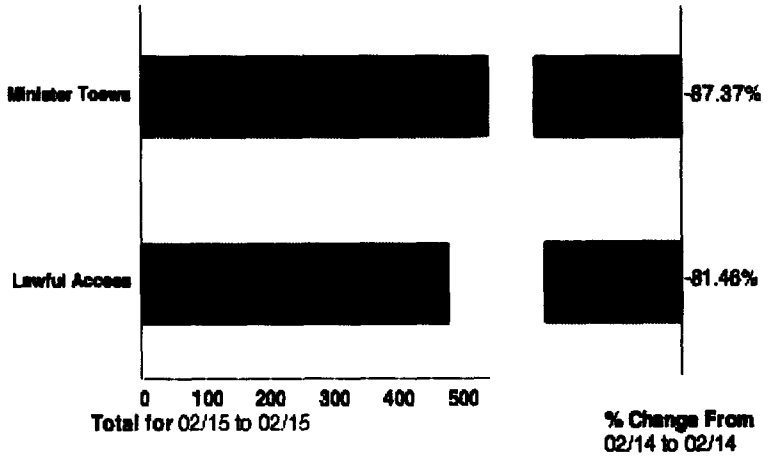
RDI présente une entrevue sur un ton négatif avec Roch Tassé, coordonnateur national de la Coalition pour la surveillance internationale des libertés civiles. Il déplore que le niveau de protection de la vie privée est moins élevé dans ce cadre que dans celui qui régit la surveillance des conversations téléphoniques. Il critique l'absence de l'obligation d'obtenir un mandat avec des standards moins élevés que présentement dans le Code criminel. Il voudrait se présenter devant un comité parlementaire. (RDI, 10 :50am)

Social Media

Overview

There has been a high volume of coverage of the Lawful Access legislation on social media channels today (February 15, 2012.)

The majority of discussion on social media continues to focus on Minister Toews specifically. A comparison graph showing the distribution of mentions the minister against mentions of Lawful Access legislation is shown directly below. The data for February 15th, shows a 80-87% decrease in discussions concerning the Minister and Lawful Access in comparison to the data from February 14th.



Mentions of Minister Toews and Lawful Access have followed the usual distribution across social media channels, with most occurring on the Twitter platform. Discussions about Minister Toews continue to show a focus on child pornography/pornographers. Keywords coinciding with mentions specifically of Lawful Access have shifted focus. "Spying" and related terminology is being discussed in relation to Bill C-30. Most mentions have been negative in tone.

Keywords coinciding with Ministerial mentions on social media:

warrant phone pornographers spy rights house
time police surveillance mps commons says
conservatives government vic video information
canada opposition minister porn canadian registry
cdnpoli internet toewsvic spying allow data
children protecting @npsteve online child canadians
stephen look law news legislation ottawa access
gun electronic safety stand toews act
public harper

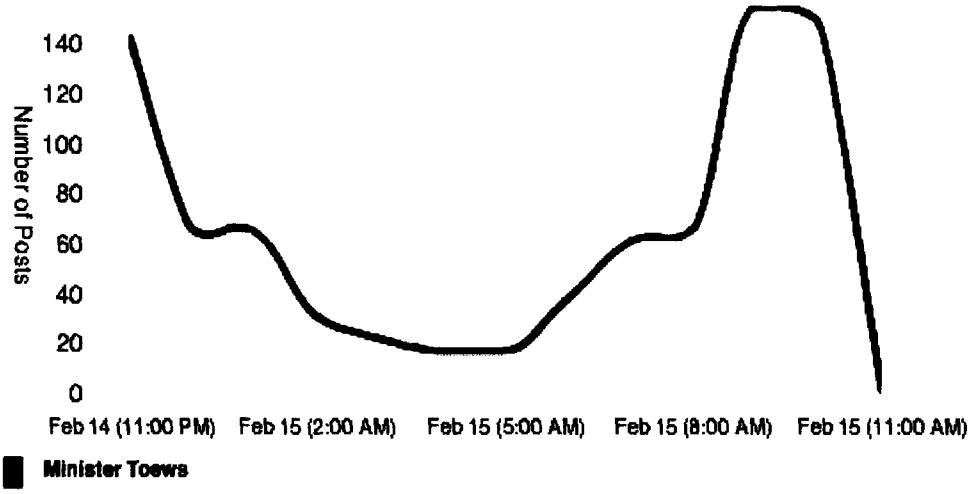
Keywords coinciding with mentions specifically of Lawful Access on social media:

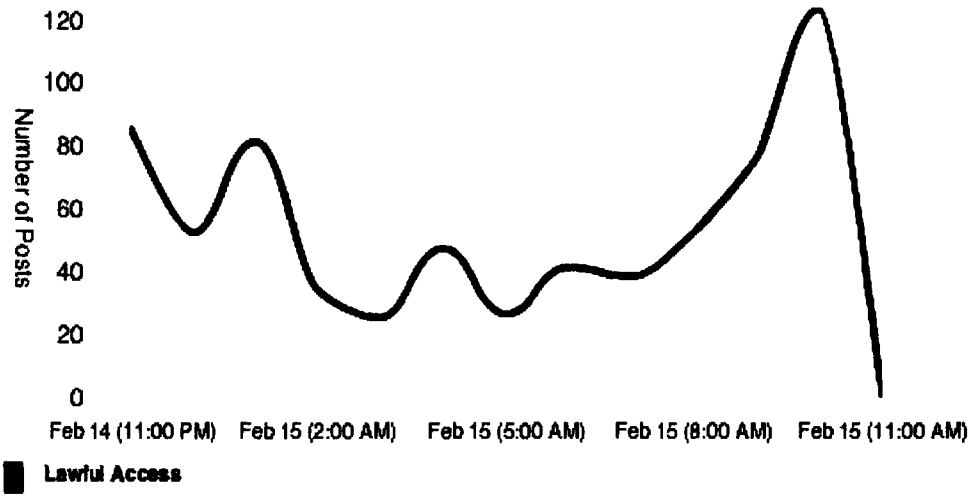
phone passed pull spy time conservative
surveillance c-30 laws government vic sopa
information **canada** national minister failure
authorities plug canadian internet #cdnpoli
online-spying powers spying children
pipa protecting online child #privacy c-51
petition canadians #canada law @mgeist news
legislation **introduces** **access**
electronic works predators toews **lawful**
prayers act harper

Trend Analysis

Mentions of the Minister decreased in the early morning hours, however a spike in activity occurred in the early morning. Since this morning, mentions of Lawful Access and Minister Toews have followed the same trend on social media.

The bulk of discussion during the spike in activity this morning appears to be the result of the publication and sharing of traditional media articles on the topic of Lawful Access:





Public activity on social media concerning Lawful Access has had several peaks with information being shared at 1:00 and 3:00 AM eastern standard time, Discussions concerning the Minister and Lawful Access was at its highest peak at approximately 9:00 AM. The following tweet and editorial cartoon were amongst the most popular information being shared referencing the Minister at that time:

Tweet:
NPsteve
WITH OR AGAINST: I look inside the mind of Vic Toews! news.nationalpost.com/2012/02/14/vic...

Editorial Cartoon:
Vic Toews: With him or against him?
news.nationalpost.com

The following tweet and blog post were amongst the most popular information being shared referencing Lawful Access at 9:00AM:

Tweet:
privacylawyer
#LawfulAccess then and now: Comparing C-52 to current C-30 bit.ly/y1M3lm #privacy #CanPoli

Blog Post:
Lawful Access then and now: Comparing C-52 to current C-20
Canadian Privacy Law Blog

Twitter

WatchCTVNews
.@cavoukian discusses how police and government have no right to access private #online data #cdnpoli ow.ly/94dwR

cancivlib
Live chat on canada.com starting at 1pm EST re: "lawful access" bill - bit.ly/zeIMAE #cdnpoli #privacy

dgardner
Remember how Vic Toews said the Canadian Bar Association and other critics of CPC crime policy are "pro-crime"? bit.ly/wdAPT7

wicary
Protecting Children from Internet Predators Act is an embarrassing failure, @thehartley writes. flpbd.it/bgwgS #cdnpoli

macleansblogs
Vic Toews parses himself: In an interview with CTV, the Public Safety Minister maintains there's a difference be... bit.ly/z58jc8

mgeist
Scanned versions of Bill C-30, the online surveillance bill: Part 1 is.gd/4t0Q7L Part 2 is.gd/nLuGzC

dgardner
Cracks in the monolith? Judging by talk radio and other conservative media, "lawful access" may be a snoop too far. bit.ly/yKj52l

mgeist
RT @privacylawyer: #LawfulAccess then and now: Comparing C-52 to current C-30 bit.ly/y1M3Im

bobraeMP
"What a difference a day makes" - Vic Toews gets his new instructions from PMO : bit.ly/ykLBVE"

dgardner
Vic Toews tries and fails to be Clintonian. bit.ly/x3zXhi

billhillier
What lawful access is all about and why it matters = is.gd/FqpRvG #cdnpoli #c30

fitzpatrick_m
Vic Toews+Candice Hoeppner+Maxime Bernier press conference now, on final day of debate+vote on gun registry #hw

kady
Meanwhile, Public Safety Minister Vic Toews is now preemptively celebrating third reading of the gun registry bill. #hw

troyrhoades
The government fights for its "lawful access" blogs.canoe.ca/davidakin/tech... #lawfulaccess

CharlieAngusMP
#lawfulaccess is lawful spying. Stock Day defended need for warrants. Toews sez times have changed. Not good enough Vic. #ndp will fight.

NPsteve
WITH OR AGAINST: I look inside the mind of Vic Toews! news.nationalpost.com/2012/02/14/vic...

danlebla
Mon collègue Bado s'est lâché lousse aujourd'hui. J'aime particulièrement son Vic Toews twitpic.com/8k8dw4

seankheraj
Great mini-doc on lawful access expansion in Canada youtu.be/xyHnOCDewuQ #lawfulaccess #stopspying

Blogs

Can you spot the difference on "lawful access" bill?
So the Conservative government sends off a contentious bill for printing and provides copies to House of Commons staff to distribute and table in Parliament — then withdrawals it an hour later and replaces with a new version? That's what happened Tuesday when Public Safety Minister Vic Toews, through the Speaker of the House, tabled the Investigating and Preventing Criminal Electronic Communications Act just after 10:00 am. The short title is listed as "Lawful Access Act." An hour later, House of Commons staff withdrawal it and replace it with the identical bill, save a new short title. It's now the "Protecting Children from Internet Predators Act." Politics and the Nation

Why a Lawful Access Compromise Can Be Found
The launch of Bill C-30, the online surveillance legislation dubbed the Protecting Children from Internet Predators Act, went about as expected with the government taken to task with big brother imagery ("Say Hello to Big Brother Government") and criticism over the lack of evidence ("Conservatives hew to common sense save for bizarre crime fixation"), the security threats ("Online surveillance bill will be 'a gold mine' for hackers: Ontario privacy commissioner"), and the absence of a thoughtful digital vision ("Canada's embarrassing failure on lawful access legislation"). The divisive comments from Public Safety Minister Vic Toews seemed to shape much of the dialogue, serving to ratchet up the rhetoric and overshadow both the modest changes to the bill and the legitimate remaining concerns of many Canadians. Michael Geist Blog

The government fights for its "lawful access"
Across our newspaper chain today, I argue that the C-30, the government's so-called "lawful access" legislation, is bad, that, "there is no excuse for this kind of intrusion on the privacy rights of Canadians and certainly not one from a government that says it champions the idea that the federal government ought to respect individual liberties and rights." [Read my full column on this]
Last night, perhaps seeing that there were a great number of pundits criticizing this bill [here's the Post's Matt Hartley, for one], one of the aides for Public Safety Minister Vic Toews circulated three examples that it believes show the need for the new powers to be given to police, CSIS, and the Competition Bureau in C-30. It doesn't change my assessment of the bill — no example is given here to support the idea in C-30 and Competition Bureau bureaucrats or spies from CSIS ought to be able to get subscriber information without a warrant – but here it is for your consideration:...On The Hill

Our moment, our Internet
As you probably noticed, the Internet is under siege from all angles at the moment. Communications seem be at a crossroads in Canada, and indeed around the world. Will we live in a connected society that respects free expression, creativity and innovation? Or will we live in country with increasingly punitively expensive access to communications with widespread censorship and surveillance?...Open Media

Lawful Access then and now: Comparing C-52 to current C-30
In case you are, like me, spending the evening checking out what has changed with respect to warrantless access to subscriber data between Bill C-52 (introduced last year) and Bill C-30 introduced in Parliament today, this redline comparison may help. Privacy Lawyer

Facebook

This article was very popular on Facebook, with many users attaching similar statements:

"We just can't let this happen, have we forgot what happened in Germany 70 years ago?"

http://business.financialpost.com/2012/02/14/comment-canadas-embarrassing-failure-on-lawful-access-legislation/

> **Comment: Canada's embarrassing failure on lawful access legislation**
> business.financialpost.com
> It's time Canadians come to grips with the unfortunate truth that the federal government simply isn't interested in demonstrating any sort of thoughtful leadership when it comes to the pressing digital issues of our day...

"Bye, bye, privacy. Canada introduces online-spying bill "

http://rt.com/usa/news/bye-canada-bill-internet-335/

> **Bye, bye, privacy. Canada introduces online-spying bill**
> **rt.com**
> Move over, SOPA and say your prayers, PIPA. There's a new bill in the works that, if passed, will pull the plug on how the Internet is used in Canada. Lawmakers in the Great White North are debating a bill that will pulverize what's left of online privacy for Canucks...

"It seems appropriate that the US fear mongering tactics are employed to bring in US anti-citizen bills. To suggest oppose to this bill is to align support with child pornographer is completely and utterly ridiculous!! Look through the smoke and stand up to this BULLY and his tactics!!"

Willey, Chris

From: Therien, Stephane on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: Tuesday, February 14, 2012 6:11 PM
To: * COMMS ADG / Bureau du directeur géneral associé; * COMMS Communication Services Division / Division des services de communication; * COMMS DGO / Bureau de la directrice générale; * COMMS Program Communications Division / Secteur des communications de programmes; * COMMS Public Affairs Division / Secteur des affaires publiques; * Speeches / Discours; Astravas, Rutha; Banerjee, Ritu; Beaudoin, Serge C; Bolton, Stephen; Boucher, Patrick; Boucher-Lalonde, Murielle; Cameron, Bud; Carmichael, Julie; Champoux, Elizabeth; Clairmont, Lynda; Coburn, Stacey; Crawford, Andrée; Csversko, Christine; Currie, St. Clair; Daoust, Normand; De Santis, Heather; Duschner, Gabrielle; Dussault, Josée; Easson, Grant; Gareau-Lavoie, Genevieve; Gordon, Robert; Hitchcock, Christy; House, Andrew; Huggins, Rachel; Humeniuk, Elena; Hunt, Ryan; Jarmyn, Tom; Johnson, Mark; Kelland, Stephen; Khouri, Lisa; Komm, Chantelle; Kubicek, Brett; Lavoie, Micheline; Leclair, Natalie; Leclerc, Carole; Leonidis, Nelly; Lesser, Robert; MacDonald, Nicholas; MacKinnon, Paul; Marchand, Renee; McAteer, Julie; Morris, Marika; Motzney, Barbara; Mundie, Robert; Nicole, Jean-Thomas; Oldham, Craig; Panthaky, Jasmine; Patton, Michael; Pozhke, Nicholas; Rosario, Giselle; Roy, Isabelle; Saunders, Joanne; Shuttle, Paul; Slack, Jessica; Thibault, Stéphane; Tupper, Shawn; Van Criekingen, Jane; Verret, Scott; Wex, Richard; Wilson, Gina; Adam.Kates@cbsa-asfc.gc.ca; Allison.Wildgust@cbsa-asfc.gc.ca; Amitha.Carnadin@cbsa-asfc.gc.ca; Bateman, Paul; Bernard.Alladin@cbsa-asfc.gc.ca; Bindman, Stephen; Brunette, Lynn; cbsa.media@cbsa-asfc.gc.ca; Cgirouad@justice.gc.ca; Chad.Fleck@international.gc.ca; Williams, Christpher; Churney, Daryl; Cocking, Marie; Couture, Jocelyne; Derek Cefaloni; Douglas, Caroline; Van Allen, Elizabeth; C. Girouard; Bradley, Jolene; Mackillop, Ken; Lamothe, Maureen; Lauzon, Raymond; Lavoie, Daniel; MacDonald, Jane; Mailhot, Esther; Stokes, Mark; Mary.Schlosser@rcmp-grc.gc.ca; RCMP Media Monitoring; Melissa Hart; Martin, Nadie; Robinson, N.; Giolti, Patrizia; Prieur, Mark; Rioux, Veronique; Rondeau, Martine; Sbinman@justice.gc.ca; Dumoulin, Stéphanie; Tim.Cogan@rcmp-grc.gc.ca
Subject: Media Snapshot: Protecting Children from Internet Predators Act / Loi sur la protection des enfants contre les cyberprédateurs, 14-02-2012

Protecting Children from Internet Predators Act / Loi sur la protection des enfants contre les cyberprédateurs
Media Snapshot | Aperçu médiatique

14-02-2012

Key issues and overview

- On Tuesday, February 14th, Public Safety Minister Vic Toews and Justice Minister Rob Nicholson tabled the "lawful access" legislation titled, *Protecting Children from Internet Predators Act,* in the House of Commons.

- This issue has received a significant amount of national and regional media attention from all media types. The vast majority of the media attention has been highly negative in tone primarily focusing on the comment Minister Toews made in the House of Commons on February 13 regarding child pornography. Twitter has been the most widely-used medium for critics to express their views of the legislation.

Quotes from the Opposition and stakeholders

"Anyone that's been around this area will know that we do not have the resources or the capacity to be monitoring randomly in any kind of a pervasive way normal communications that occur between citizens of this country. We're targeting people who are engaged in the distribution and production of child pornography, that are involved in serious

organized crime and those kinds of activities. We just don't have the capacity to go beyond that." **~Tom Stamatakis, President, Canadian Police Association,** (Media availability, 2012-02-14, 13h30 ET)

"This bill isn't going to change the ability of a person acting unlawfully to take a step that isn't available to them in the law. I would suggest that would be extremely rare in this country but if it happens this bill isn't going to prevent it or it's not going to assist it. If you're talking about free expression this bill isn't going to impact on who is appropriately a target of a police investigation. Obviously in this country you have to have committed a crime and there has be to be at least reasonable grounds to suspect, or reasonable grounds to believe before the police can take these kinds of steps. This bill for example as I understand it even increases the threshold on us to get a tracking device. Previously we could apply for a tracking device on the basis of reasonable grounds to suspect. We're advised that this threshold has been increased to reasonable current grounds to believe and this is a higher standard to meet." **~ Murray Stooke, Deputy Chief, Calgary Police Force** (Media availability, 2012-02-14, 13h30 ET)

"I've got a couple of concerns. But heading up at the very top of the list is this mandatory disclosure of subscriber information without a warrant. The reality is today that the internet providers, telecom companies can disclose that information as part of an investigation, but aren't mandated to do so. And, in fact, most of the time, the overwhelming majority of the time, they do disclose. According to data from the RCMP, about 95% of the requests where they request for subscriber information are met on a voluntary basis. We're really just talk about the last 5%. And for that last 5% what happens is you get an ISP or a telecom company that says you know what? I'd be more comfortable if you came back with a warrant and I'll provide you with whatever information you like. That's the kind of privacy protection that exists within the law today. It's the kind of privacy protection that courts who have looked at this issue in any number of different cases, not just in crime cases, but also dealing with copy right and the like, have said that's how we try to strike a balance. And what the government is doing with this legislation is throwing that balance out entirely. Saying that there can be mandated disclosure, no court orders". **~ Michael Geist, (CTV News, 2012-02-14, 16h10 ET)**

"Now, every single Canadian citizen is walking around with an electronic prisoner's bracelet. I say to Vic Toews, 'Stop hiding behind the boogey man. Stop using the boogey man to attack the basic rights of Canadian citizens.' Is Vic Toews saying that Stockwell Day supports child pornography? Is Vic Toews saying that every privacy commissioner in this country who has raised concerns about this government's attempt to erase the basic obligation to get a judicial warrant, is he saying that they're for child pornography?" **~ NDP MPs Charlie Angus** (National Post, 2012-02-14, 15:29 ET)

"Exactly, this bill – and in cases where there's imminent threats of terrorism for instance, the police already have the ability to get whatever they want quickly. That already exists in law. So what we're looking at here is, and I await what the privacy commissioners will believe about the extent of the information, they did answer questions that with a cellular telephone address, and access to that information, they would still require one step more to begin to track someone's movements based on their cell phone. That would still require a warrant. So I look forward to the debates and the committee process, but I'm really quiet worried of the extent of information that they will - that will be available to law enforcement authorities without any warrant and without any suspicions against anyone." **~ Elizabeth May, Leader, Green Party of Canada** (Media availability, 2012-02-14, 10h55 ET)

"I don't like the idea of anybody checking up on me whether I'm guilty or not. I mean if I'm guilty, you know, I accept it, that they're doing – that they're doing their job, but if I'm not guilty and I discover that somebody's snooping on me, I find that – I mean we're not living in a totalitarian state. We're not living in the 1984 scenario. We do believe in freedoms in this country and things have to be done, yes, crime has to be pursued, but it has to be done in a reasonable and in a way that – that it holds even the police to account." **~ Marc Garneau, Liberal MP** (Media availability, 2012-02-14, 10h45 ET)

Print Media

Print media coverage leading up to the announcement

Tories stand firm on 'lawful access' legislation

The "lawful access" legislation, to be tabled in the House of Commons on Tuesday, means Internet service providers and cell phone companies won't be able to say no if law enforcement asks them to hand over basic subscriber information of their customers. Some smaller changes are expected in the bill that could affect the oversight model and internal controls, but **Public Safety Minister Vic Toews** has stood firm on the broad strokes, saying new measures are needed to catch criminals in the 21st century, singling out child pornography cases. **Canada's privacy commissioners** banded together last year to write an open letter to Toews, saying police shouldn't have unrestricted access to basic subscriber information

held by telecommunications companies. But senior departmental officials also criticized Toews, who previously served as attorney general of Canada and Manitoba, for failing to state in his public response to Cavoukian that there are provisions of the Criminal Code that allow police to read emails without a warrant. While Toews publicly says the bill is designed to go after users of child pornography, internal records refer to other issues, says **Michael Geist**. "You just can't be serious. On one hand, we'd got Vic Toews screaming about child pornography cases and on the other hand, it's pretty clear that one of their main justifications is that this has to do with non-emergency situations that aren't even criminal situations. To say that you're going to drop key privacy protections because you want to return a kid's bike is just absurd," Geist said. Ottawa Citizen, A1 (Starphoenix, Leader-Post, Montreal Gazette, Windsor Star, Edmonton Journal, Vancouver Sun, Calgary Herald, Times & Transcript, The Province, Times Colonist, Daily Gleaner, Winnipeg Free Press)

Toews says bill opponents side with child pornographers
The government says anyone who opposes federal plans to make electronic surveillance easier for police and spies is siding with child pornographers. It's the first salvo in a battle that will resume Tuesday when the government reintroduces legislation that would expand online monitoring powers. Asked Monday in the House of Commons about the coming bill, **Public Safety Minister Vic Toews** told a Liberal MP he could either stand with the government or "with the child pornographers" prowling online. **Toews' office** has said the government will strike an appropriate balance between necessary investigative powers and the protection of privacy. Still, opposition MPs were alarmed by Toews' comments Monday. Toronto Star, A8 (Hamilton Spectator, The Telegram, Chronicle-Herald); Le Devoir

Tories introduce 'lawful access' bill
INTERNET: The Tories table contentious "lawful access" legislation in the House of Commons today. If passed, law enforcement officials could impel Internet service providers and cell phone companies to turn over basic subscriber information about their clients. Calgary Herald, A2

A licence to snoop
An editorial states, "But while the government restores some of our freedoms with one hand, it simultaneously takes them away with the other. Public Safety Minister Vic Toews has placed the Conservatives' so-called "lawful access" legislation - which they've been trying to pass since 2009 - on the House of Commons Order Paper...The Conservatives have been intent on enacting laws that give more power to police and impose a heavy burden on society, despite a lack of evidence of the effectiveness of such measures. Should our government be vigorously combating such evils as terrorism and child pornography? Of course. But it must find a way to do so without sacrificing Canadians' basic civil liberties in the process." National Post, A12

Online Media

Online media coverage was extensive and negative in tone. Coverage focused on the new legislation that would make it easier for law enforcement to conduct electronic surveillance. The official Opposition and stakeholders stated there is no justification for the legislation citing privacy concerns.

Online surveillance bill will fight cyber crime: minister
Justice Minister Rob Nicholson says new legislation that would make it easier for law enforcement to conduct electronic surveillance will allow police and other agencies to "to fight crime in the 21st century. Nicholson said new legislation tabled Tuesday, called the "Protecting Children from Internet Predators Act," is a response to rapid changes in technology available to criminals, with which legislation and the Criminal Code have not kept up . . . **Public Safety Minister Vic Toews** said the bill, among other things, will require telecommunications service providers to implement and maintain systems by which they can monitor and intercept communications, as well as systems to allow them to more quickly respond to requests for information from law enforcement agencies. But he said the bill does not allow the government to monitor private communication, Web activity or emails of Canadians. And it will not allow police to look at the substance of en email without a warrant. CTV News; CBC News; Canadian Press; Montreal Gazette

Ottawa veut faciliter l'accès aux communications électroniques pour les policiers
Le gouvernement Harper veut permettre aux services de police, aux services secrets et aux enquêteurs du Bureau de la concurrence d'obtenir sans mandat les données personnelles des d'internautes auprès des fournisseurs de service de téléphonie et d'Internet. Des dispositions en ce sens se retrouvent dans le projet de loi C-30 sur la protection des enfants contre les cyberprédateurs, présenté mardi à la Chambre des communes par les ministres de la Justice et de la Sécurité publique, respectivement Rob Nicholson et **Vic Toews**. Radio-Canada ; TVA Nouvelles; La Presse Canadienne; AFP

Opposition blasts e-snooping bill
The official Opposition mounted a quick counter attack against the government's lawful access bill Tuesday, calling it a "spy bill" that proves the Conservatives have shallow concern for privacy. "Canadians are not criminals," Charlie Angus

said, echoing the Conservative government's own reasoning on scrapping the long-gun registry. iPolitics; Global News; News1010

Online surveillance bill critics are siding with 'child pornographers': Vic Toews
Opponents of a controversial bill that would give authorities new powers to increase online monitoring of Canadians have been accused of siding with "child pornographers" by **Safety Minister Vic Toews**. The so-called "lawful access" legislation, tabled in the House of Commons on Tuesday and expected to pass under a Conservative majority government, means Internet service providers and cellphone companies must hand over basic subscriber information of customers to law enforcement agencies. Opponents of the proposed law claim it is 'untenable', but Mr. Toews said yesterday that people ***"can either stand with us or with the child pornographers."*** National Post

New 'lawful access' law could amount to illegal search and seizure
Lawful access or unlawful access? Critics of the federal government's proposed bill that will give police increased access to customer data from Internet service providers, predict there could be constitutional challenges to the legislation down the road. Bill C-30, the proposed "protecting children from Internet predators act" was introduced today. It contains provisions from previous bills C-50, C-51 and C-52 that raised the concerns of privacy watchdogs. Canadian Lawyer Magazine

Lawful Access: a creepy Valentine from Vic Toews
An editorial piece states, "Vic Toews wants to make one thing clear: He does not want to read my email. His office reached out to me after I wrote this post, which detailed the inability of our police to find one good example of why they need new Lawful Access laws, to be tabled today..." Maclean's

Is Vic Toews against freedom?
An opinion piece states, "It's hard to imagine what points **Public Safety Minister Vic Toews** thinks he is scoring when he describes those concerned about the implications of increased government Internet surveillance as supporting child pornographers..." ITBusiness

'With us or with the child pornographers' doesn't cut it, Mr. Toews
An editorial piece states, "What you think of the Conservatives' new bill to expand police surveillance of the web may depend on what you think of the long-gun registry and the long-form census. Public Safety Minister Vic Toews will argue that the new legislation, to be introduced Tuesday afternoon, will grant the government access to nothing more than the Internet equivalent of a telephone book, which police need to help track criminals and terrorists..." Globe and Mail

Warrantless Access Unjustified in Surveillance Bill
An opinion piece states, "As Public Safety Minister Vic Toews proclaims in the House of Commons that you either support lawful access or stand with child pornographers, Sarah Schmidt of Postmedia had a great story yesterday afternoon on new lawful access revelations obtained under the Access to Information Act..." Huffington Post

National Post: Even officials from Public Safety Canada take issue with online spying
An opinion piece states, "For years, small-c conservatives have been arguing that the gun registry is a giant waste of money — not only because it went way over budget, but due to the fact that it serves to make criminals out of law abiding firearms owners..." Open Media

Should police have access to ISP customer data without a warrant?
The Conservative government is expected to introduce a bill Tuesday to give police new powers to access Canadians' electronic communications. The "lawful access" bill is expected to include provisions that were included in previous bills that died when last year's election was called. CBC News

Broadcast Media

Broadcast media attention was extensive and negative in tone. Reports focused on Minister Toews' comments from the previous day and privacy concerns regarding the new bill.

Broadcast media reported the government will reintroduce Lawful Access legislation today. (CKQM-FM, Peterborough, 5:01am; Mix News, CIGL-FM, Belleville, 6:01am; CJBK-AM, London, 6:02am; CFTR-AM; The Dawg's Breakfast, CIDG-FM, Ottawa, 6:31am, 7:27am; Moore in the Morning, CFRB-AM, Toronto, 6:04am; 95 Second Update, CJOJ-FM, Belleville, 6:30am, 7:02am; The Morning News Wheel, CKPC-AN, Brantford, 8:00am; BOB-FM, CKLY-FM, Lindsay, 8:02am; CP24, Toronto, 11:30am; CTV News at Noon, CKY-TV, Winnipeg, 12:11pm; CJOH-TV, CTV Ottawa, 12:34pm; CFRN News, CTV Edmonton, 12:00pm)

Broadcast media reported Minister Vic Toews said either side with the government on Lawful Access legislation or side with child pornographers. (On Target Ottawa, CFRA-AM, Ottawa, 5:02am, 5:11am; CILV-FM, Ottawa, 6:02am; CJBQ-AM, Belleville, 6:01am; CKRU-FM, Peterborough, 6:02am; CJWL-FM, Ottawa, 6:31am; CKWS-FM, Kingston, 7:00am; CKAP-FM, Kapuskasing, 7:01am; CJTT-FM, New Leskeard, 7:01am; Perspective, CHRI-FM, Ottawa, 7:01am; MYFM News, CKYM-FM, Napanee, 7:00am; The Breakfast Club, CFJR-FM, Brockville, 7:02am; CJCS-AM, Stratford, 8:01am; Rock 107 News, Belleville, 8:00am; CKGL-AM, Kitchener, 8:08am; Tom McConnell Show, CKTB-AM, St. Catherines, 10:02am; CHAN-TV, Global Vancouver; CTV News at Noon, CFTO-TV, Toronto, 12:13pm; CTV News Channel, 03:30pm)

The Gary Doyle Show discussed the Lawful Access bill and took calls from listeners about the subject (Gary Doyle Show, CKGL-AM, Kitchener, 12:03pm)

CTV News presented live coverage of a news conference by NDP MPs Charlie Angus, Jasbir Sandhu, and Charmaine Borg on the Lawful Access bill. They disapprove of the bill because of privacy concerns and on the grounds that law abiding Canadians should not be treated as criminals. (CTV News, 10:30am) Rough transcript

CTV News reported that with his comments that you can either stand with the government or "with the child pornographers" prowling online, Public Safety Minister Vic Toews has, "almost single-handedly united everyone against him and almost everybody against the legislation." (CTV News, 11:30am)

CTV News reported **Minister Toews' office** has said the government will strike an appropriate balance between necessary investigative powers and the protection of privacy. (CTV News, 11:30am)

CBC News noted that when Stockwell Day was Minister of Public Safety in 2007, he said that he would not require ISP disclosure without a warrant. (CBC News, 12:00pm)

SUN-TV discussed the Lawful Access bill, Minister Toews' comments and questions of privacy (SUN-TV, Toronto, 11:49am)

SUN-TV asked **Minister Toews** if he wanted to rethink his comments from the previous day. According to SUN-TV, **Minister Toews** said that he never accused anyone of supporting child pornographers and that's not what he feels. He did say that the bill is necessary to fight the proliferation of pornography and organized crime (SUN-TV, 3:05pm)

CBC News and CTV News presented live coverage of a news conference by **Minister of Public Safety Vic Toews**, Minister of Justice Rob Nicholson and Senator Jean-Guy Dagenais to announce the Protecting Children from Internet Predators Act. (CBC News, CTV News, 12:45pm) CTV News Rough Transcript, CBC News Rough Transcript

CBC News showed a clip of Question Period in which **Minister Toews** stated:" Mr. Speaker, I can say that is false. There's nothing in the bill that allows police to snoop on private individual conversations or follow activity on the web. It has to be done through a judicially authorized warrant and had he stayed for the technical briefing that was provided for him, he would have in fact have heard that." (CBC News, 03:30pm)

CTV News interviewed Michael Geist regarding the Protecting Children from Internet Predators Act. The Minister was mentioned in this interview. Rough Transcript

CTV News – Power Play interviewed **Public Safety Minister Vic Toews** regarding the Protecting Children from Internet Predators Act. Rough Transcript

CBC News – Power & Politics interviewed **Public Safety Minister Vic Toews** regarding the Protecting Children from Internet Predators Act. Rough Transcript

CBC News – Power & Politics interviewed MPs Charlie Angus and Francis Scapaleggia regarding the Protecting Children from Internet Predators Act. The Minister was mentioned several times in this interview. Rough Transcript

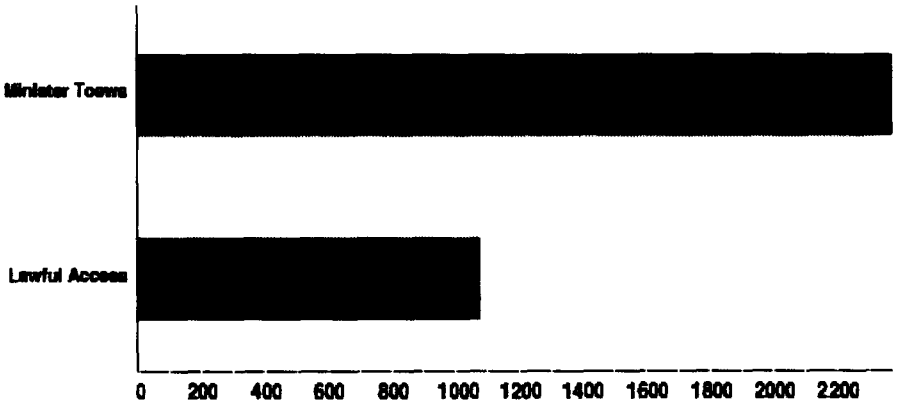
CTV News – Power Play interviewed Chantal Bernier, the Assistant Privacy Commissioner, regarding the Protecting Children from Internet Predators Act. The Minister was mentioned in this interview. Rough Transcript

Social Media

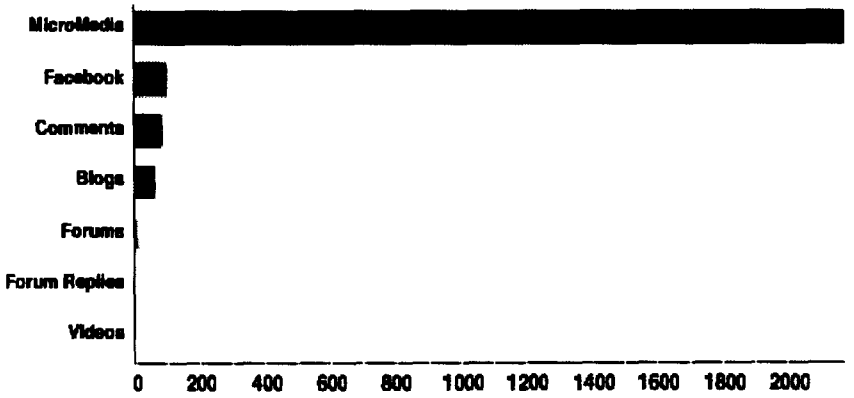
Overview

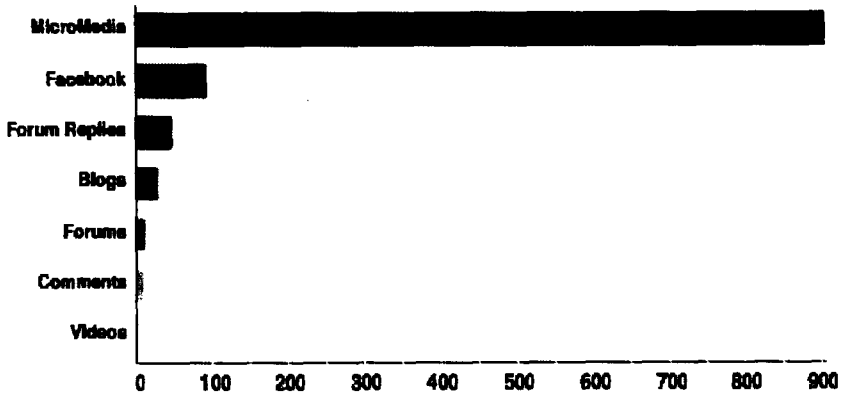
There has been a high volume of coverage of the Lawful Access legislation on social media channels today (February 14, 2012.) In comparison with other issues relevant to Public Safety Canada in previous analyses, the coverage is approximately four to five times the volume.

Most of the discussion has mentioned Minister Toews specifically. A comparison graph showing the distribution of mentions the minister against mentions of Lawful Access legislation is shown directly below:



Mentions of Minister Toews and Lawful Access have followed the usual distribution across social media channels, with most occurring on the Twitter platform.





Discussions about Minister Toews and Lawful Access show a focus on child pornography/pornographers. Most mentions have been negative in tone.

Keywords coinciding with Ministerial mentions on social media:

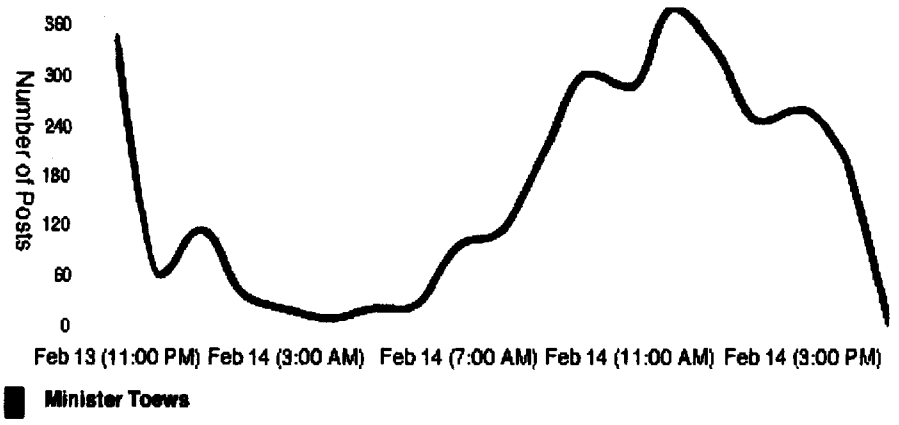
Keywords coinciding with mentions specifically of Lawful Access on social media:

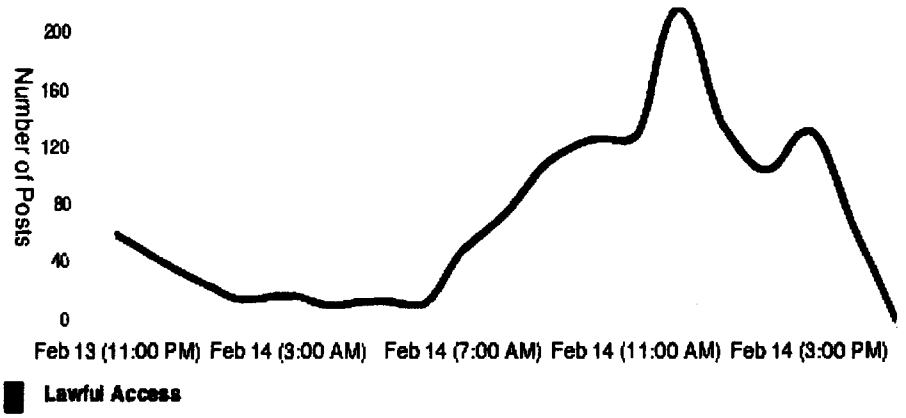
Trend Analysis

Mentions of the minister spiked last night as users took to social media to discuss the statements made regarding child pornographers. Since this morning, mentions of Lawful Access and Minister Toews have followed the same trend on social media.

The bulk of discussion during the spike in activity last night appears to be the result of the sharing of the following tweet:

> **Bill Hillier @billhillier**
> Do you agree with the statement made by **@ToewsVic** 'Stand with us or with the child pornographers' **#cdnpoli**





Public activity on social media surrounding the Minister and Lawful Access legislation was at its highest peak at approximately 12:00 PM. The focus of discussion at this point in time was about the declaration that siding against Lawful Access would mean siding on the side of child pornographers. The following tweet and article were amongst the most popular information being shared at that time:

> **Tweet:**
> Niraj Rajput @nirajrajput88
> Canadian MP: if you oppose warrantless snooping, you \"stand with child pornographers\": **Vic Toews**, the Canadian...
> http://bit.ly/zuleE4
>
> **Article:**
> Vic Toews accuses online surveillance bill C-51 opponents of siding with 'child pornographers' | New
> news.nationalpost.com
> The bill in question, to be tabled in Parliament on Tuesday, would require telecommunications companies to cough up customer inf0rmation to police without a court order.

Since 12:00 PM, the public discussion has slowly begun to recede. It's expected that coverage will spike again with more sharing in the form of blog posts containing opinions on the legislation.

Twitter

OpenMedia_ca
Could happen, we guess. ET @RobTrewartha: If Vic Toews gets his way Rogers will be able to charge an "Internet Eavesdropping" fee. #cdnpoli

OpenMedia_ca
Bang on: @CharlieAngusMP "I think Vic Toews has besmirched his reputation" ow.ly/94lhi #cdnpoli #stopspying #stopc11

kady
Mauril Belanger up on a pt of order demanding Vic Toews apologizes for his suggestion that opponents to C-30 side w/child pornographers #hw

kady
You know, I'm betting he'll decline to disclose that. @KevinSMcArthur: Hey @kady please ask Vic Toews for his home IP address.

CharlieAngusMP: Do u think cops should be able to spy on your internet and track your cellphone without warrant? Vic Toews promotes #lawfulaccess snoop bill

jonpetrychyn
If this goes through (and it will) you might as well say goodbye to internet privacy and security. bit.ly/wF0xLK

MikeRadoslav 4:45pm via web
Vic Toews said if you don't support strict online surveillance you side with child pornographers. tinyurl.com/7frxvyb #cdnpoli

delmarhasissues
Vic Toews, Conservative Minister in charge of fear mongering: "Stand with us or with the child pornographers." Ass. theglobeandmail.com/news/politics/...

canadiancynic
If Vic Toews gets his warrantless online surveillance, and child pornography continues, can we hold him *personally* responsible?

adamriggio
I can't believe Vic Toews whipped out the If-You-Have-Nothing-to-Hide-You-Have-Nothing-to-Fear logic to justify mass online surveillance.

kayoazuL
Authoritarianism creeps into culture of Harper governmentharperindex.ca/ViewArticle.cf...#CAIRS #cdnfascism #cdnpoli Vic Toews

thehartley
FP Tech Desk Comment: Canada's embarrassing failure on lawful access legislation #cdntech #cdnpoli natpo.st/w49jNn

totalservicepro
Government unveils new lawful access legislation: The Harper government has introduced its long-awaited lawful a... bit.ly/zxWLBT

RosieBarton
Toews is saying Evan is torquing up the rhetoric.

PnP_CBC
#PNP #Ballotbox Are you worried about your privacy with the new internet bill? Vote here: on.fb.me/xlJqlX #cdnpoli

JasonMagder
Love children? You must hate privacy, says public safety minister Vic Toews | Montreal Gazette fb.me/Lg08kZbe

yorandomtweeter
Vic Toews might single-handedly destroy the entire Canadian telecom sector with #BillC30. #cdnpoli

AntoniaZ
You're either with us or with the child pornographers. natpo.st/xtlFLv #cdnpoli #C130 #GiveUsABreak

canadiancynic
Dear "Anonymous" hackers: If the Cons' "lawful access" legislation passes, I'll want to know where Vic Toews has been online. Hugs, CC.

citizenlab

thehartley writes scathing critique of #LawfulAccess in today's Fin Post natpo.st/y1Xz4z via @RonDeibert #stopspying

Blogs

National Post: Even officials from Public Safety Canada take issue with online spying
For years, small-c conservatives have been arguing that the gun registry is a giant waste of money — not only because it went way over budget, but due to the fact that it serves to make criminals out of law abiding firearms owners. Meanwhile, those intent on committing crimes easily escape its grip. To their credit, the federal Tories are in the process of scrapping the registry. But while the government restores some of our freedoms with one hand, it simultaneously takes them away with the other. http://openmedia.ca/blog

Montreal City Weblog
These are the depths to which our political discourse has sunk: defenders of online privacy are aligning themselves with child pornographers, according to Public Safety Minister Vic Toews. Commentary from a Globe & Mail editorialist. http://w5.montreal.com/

Toews Has Been Smearing Online Surveillance Critics For Weeks
Public Safety Minister Vic Toews' shocking comments on critics of online surveillance in the House of Commons yesterday have attracted widespread media attention with coverage in the Globe, CBC, and Postmedia. Michael Geist

If I have nothing to hide, I have nothing to fear
The response to **Vic Toews'** latest inane (insane?) ramblings has been interesting. His stupid (What else could you call it?) comment in the House of Commons that people people "can either stand with us or with the child pornographers" is really beyond the pale. This was his reasoned response to a very legitimate concern that the lawful access bill his government is aggressively pushing forward is an infringement on privacy rights, and that police agencies should not be able to breach a Canadian's privacy without, at the very least, having to show just cause and obtaining a warrant to do so. http://viewsfromthelake-eh.blogspot.com

Conservatives to Canadians on e-snooping: "Stand with us or with the child pornographers"
After reading about it in The Globe & Mail 'Stand with us or with the child pornographers', I wrote the following to my MP: The long-form census was intrusive into the privacy of Canadians, but cyber snooping is A-OK. Justification: "Stand with us or with the child pornographers". Conservatives are often accused of not being terribly bright, binary thinkers: "take it or leave it" "my way or the highway" "like it or lump it" "Stand with us or with the child pornographers". I don't subscribe to such stereotypes because they divert from the real conversation -- which centers on the dearth of integrity among most politicians, regardless of party affiliation or IQ. http://hotdogfactory.blogspot.com

Facebook

The Occupy Canada Facebook account has shared a wall-photograph which contains an adjacent description linking to multiple articles mentioning Lawful Access.

This article was very popular on Facebook, with many users attaching similar statements:

"Big Brother is coming to an ISP near you. Write your MLA today and put the brakes on this before it's too late."

http://news.nationalpost.com/2012/02/14/online-surveillance-bill-critics-are-siding-with-child-pornographers-vic-toews/

> **Vic Toews** accuses online surveillance bill C-51 opponents of siding with 'child pornographers' | New
> news.nationalpost.com
> The bill in question, to be tabled in Parliament on Tuesday, would require telecommunications companies to cough up customer inf0rmation to police without a court order.

"Uh-oh #2: **Public Safety Minister Vic Toews** says that opponents of federal online surveillance are "siding with child pornographers." "

http://www.huffingtonpost.ca/2012/02/13/online-surveillance-child-porn-toews_n_1274900.html?ref=canada

Online Surveillance Critics Siding With Child Porn: Toews
www.huffingtonpost.ca
Critics of a bill that would give law enforcement new powers to access Canadians' electronic communications are aligning themselves with child pornographers, Canada's public safety minister says. "He can either stand with us or with the child pornographers," Vic Toews said of Liberal publ...

""lawful access" provisions would...
Require internet service providers to give subscriber data to police and national security agencies without a warrant, including names, unlisted phone numbers and IP addresses.
Force internet providers and other makers of technology to provide a "back door" to make communications accessible to police.
Allow police to get warrants to obtain information transmitted over the internet and data related to its transmission, including locations of individuals and transactions.
Allow courts to compel other parties to preserve electronic evidence"

Online surveillance critics siding with child porn: Toews - Technology & Science - CBC News
www.cbc.ca
Critics of a bill that would give law enforcement new powers to access Canadians' electronic communications are aligning themselves with child pornographers, Canada's public safety minister says.

"Who voted for this party? disgraceful legislation - using the pedophile issue to intrude on the liberty of law abiding canadians. you know, it would be much easier if stevie and his band of merry idiots just introduced the 'thought police.'"

'With us or with the child pornographers' doesn't cut it, Mr. Toews
www.theglobeandmail.com
What you think of the Conservatives' new bill to expand police surveillance of the web may depend on what you think of the long-gun registry and the long-form census

Jesse Kline: Lawful access bill set to become the new gun registry
www.nationalpost.com
For years, small-c conservatives have been arguing that the gun registry is a giant waste of money — not only because it went way over budget, but due to the fact that it serves to make criminals out of law abiding firearms owners. Meanwhile, those intent on committing crimes easily escape its grip....

"http://stopspying.ca/ - How far will Harper and their government overspend to achieve a fascist Canada? Do they truly believe Canada is a wasteland of terrorist, porn guzzling, pirating, mafia members or are they simply using false dichotomy to execute their repeal of personal freedom and privacy."

Stop Online Spying
openmedia.ca
The government is trying to ram through an anti-Internet set of electronic surveillance laws that will invade your privacy and cost you money. The plan is to force every phone and Internet provider to surrender our personal information to "authorities" without a warrant.

"It seems appropriate that the US fear mongering tactics are employed to bring in US anti-citizen bills. To suggest oppose to this bill is to align support with child pornographer is completely and utterly ridiculous!! Look through the smoke and stand up to this BULLY and his tactics!!"

"Hey remember that time in 2012 when the Canadian Government was stupid enough to think that they could pass laws that allow police to have access to all our activity and information online and there be no repercussions?"

Durand, Stéphanie

From: Durand, Stéphanie
Sent: Thursday, October 04, 2012 12:57 PM
To: Carmichael, Julie; McGrath, Andrew
Cc: Swift, Andrew; Carta, John; Manji, Natasha; Binnie, Kate; Salewski, Shawn
Subject: Re: CACP video - lawful access

I informed them of direction.
I'll confirm.

From: Carmichael, Julie
Sent: Thursday, October 04, 2012 10:22 AM
To: Durand, Stéphanie; McGrath, Andrew
Cc: Swift, Andrew; Carta, John; Manji, Natasha; Binnie, Kate; Salewski, Shawn
Subject: RE: CACP video - lawful access

Did we receive confirmation from the RCMP that they will not participate in this?

From: Carmichael, Julie
Sent: October-01-12 3:40 PM
To: Durand, Stéphanie; McGrath, Andrew
Cc: Swift, Andrew; Carta, John; Manji, Natasha; Binnie, Kate; Salewski, Shawn
Subject: Re: CACP video - lawful access

Not approved

Julie Carmichael
Director of Communications
Office of the Minister of Public Safety
Julie.carmichael@ps-sp.gc.ca

From: Durand, Stéphanie
Sent: Monday, October 01, 2012 03:26 PM
To: Carmichael, Julie; McGrath, Andrew
Cc: Swift, Andrew; Carta, John; Manji, Natasha; Binnie, Kate; Salewski, Shawn
Subject: FW: CACP video - lawful access

See below. Further to our chat last week on this. VPD, as chair of the CACP is leading and have reached out to other CACP partners such as the OPP, Montreal police and others to feature officers reading script that debunks some myths. The video is designed to try to give a police explanation of some of the issues being publicly debated on lawful access.

RCMP would still like to proceed and take part in the video. Attached is the script they would use. RCMP understands that this would likely not be approved. Please advise.
I am trying to get a copy of the overall script for the video. RCMP is following-up on this to give you more context....

Thanks.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Joe De Mora [mailto:Joe.deMora@rcmp-grc.gc.ca]
Sent: Monday, October 01, 2012 12:56 PM
To: Durand, Stéphanie
Cc: Swift, Andrew; Salewski, Shawn; Christina Cefaloni; Joanna Polito; Julie Gagnon
Subject: CACP video - lawful access
Stephanie,

Further to our discussions on this subject last week, the RCMP has decided to join the four other invited agencies to participate in a CACP-led video project aimed at providing a police explanation of lawful access. Specifically, it intends to clarify some of the misinformation out there about the tools this initiative would give law enforcement. As you know this is an extremely important topic for the policing community and one that has been met with some vocal public resistance, fueled by a broad misunderstanding and lack of information about what it is and what it isn't. Even if timelines may have shifted in the legislative process, it is important to get the policing side of the story out there along with other very credible partners in law enforcement. In fact, the timing is opportune to inform the public debate now, before the misinformed debate re-ignites and we or the government are faced with having to be on the defensive.

The script of the video is not argumentative but instead focuses on providing facts. It does not confront the government but debunks some of the fallacies that are being communicated by vocal interest groups.

Please find attached the script that we suggest be read by an RCMP spokes as part of the project.

Best

Joe

Durand, Stéphanie

From: Durand, Stéphanie
Sent: Tuesday, October 02, 2012 9:24 AM
To: Daniel.Lavoie@rcmp-grc.gc.ca
Subject: FW: CACP video - lawful access

As discussed.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Carmichael, Julie
Sent: Monday, October 01, 2012 3:40 PM
To: Durand, Stéphanie; McGrath, Andrew
Cc: Swift, Andrew; Carta, John; Manji, Natasha; Binnie, Kate; Salewski, Shawn
Subject: Re: CACP video - lawful access

Not approved

Julie Carmichael
Director of Communications
Office of the Minister of Public Safety
Julie.carmichael@ps-sp.gc.ca

From: Durand, Stéphanie
Sent: Monday, October 01, 2012 03:26 PM
To: Carmichael, Julie; McGrath, Andrew
Cc: Swift, Andrew; Carta, John; Manji, Natasha; Binnie, Kate; Salewski, Shawn
Subject: FW: CACP video - lawful access

See below. Further to our chat last week on this. VPD, as chair of the CACP is leading and have reached out to other CACP partners such as the OPP, Montreal police and others to feature officers reading script that debunks some myths. The video is designed to try to give a police explanation of some of the issues being publicly debated on lawful access.

RCMP would still like to proceed and take part in the video. Attached is the script they would use. RCMP understands that this would likely not be approved. Please advise.

I am trying to get a copy of the overall script for the video. RCMP is following-up on this to give you more context....

Thanks.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Joe De Mora [mailto:Joe.deMora@rcmp-grc.gc.ca]
Sent: Monday, October 01, 2012 12:56 PM
To: Durand, Stéphanie
Cc: Swift, Andrew; Salewski, Shawn; Christina Cefaloni; Joanna Polito; Julie Gagnon
Subject: CACP video - lawful access
Stephanie,

Further to our discussions on this subject last week, the RCMP has decided to join the four other invited agencies to participate in a CACP-led video project aimed at providing a police explanation of lawful access. Specifically, it intends to clarify some of the misinformation out there about the tools this initiative would give law enforcement. As you know this is an extremely important topic for the policing community and one that has been met with some vocal public resistance, fueled by a broad misunderstanding and lack of information about what it is and what it isn't. Even if timelines may have shifted in the legislative process, it is important to get the policing side of the story out there along with other very credible partners in law enforcement. In fact, the timing is opportune to inform the public debate now, before the misinformed debate re-ignites and we or the government are faced with having to be on the defensive.

The script of the video is not argumentative but instead focuses on providing facts. It does not confront the government but debunks some of the fallacies that are being communicated by vocal interest groups.

Please find attached the script that we suggest be read by an RCMP spokes as part of the project.

Best

Joe

Durand, Stéphanie

From: Durand, Stéphanie
Sent: Monday, October 01, 2012 5:44 PM
To: 'Daniel.Lavoie@rcmp-grc.gc.ca'; 'Joe.deMora@rcmp-grc.gc.ca'
Cc: Swift, Andrew; Carta, John; Binnie, Kate; Salewski, Shawn; 'Christina.Cefaloni@rcmp-grc.gc.ca'; 'joanna.polito@rcmp-grc.gc.ca'; 'julie.gagnon@rcmp-grc.gc.ca'
Subject: Re: Rép. : RE: CACP video - lawful access

RCMP participation is not approved by the MO.

From: Daniel Lavoie [mailto:Daniel.Lavoie@rcmp-grc.gc.ca]
Sent: Monday, October 01, 2012 05:41 PM
To: Durand, Stéphanie; Joe De Mora <Joe.deMora@rcmp-grc.gc.ca>
Cc: Swift, Andrew; Carta, John; Binnie, Kate; Salewski, Shawn; Christina Cefaloni <Christina.Cefaloni@rcmp-grc.gc.ca>; Joanna Polito <Joanna.Polito@rcmp-grc.gc.ca>; Julie Gagnon <julie.gagnon@rcmp-grc.gc.ca>
Subject: Rép. : RE: CACP video - lawful access

Meaning not yet approved or that they do not approve of the RCMP participating to the video?

>>> Durand, Stéphanie<Stephanie.Durand@ps-sp.gc.ca> 2012-10-01 17:33 >>>

MO has advised that this is not approved.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Durand, Stéphanie
Sent: Monday, October 01, 2012 2:24 PM
To: 'Joe.deMora@rcmp-grc.gc.ca'
Cc: Swift, Andrew; Salewski, Shawn; 'Christina.Cefaloni@rcmp-grc.gc.ca'; 'joanna.polito@rcmp-grc.gc.ca'; 'julie.gagnon@rcmp-grc.gc.ca'; 'Daniel.Lavoie@rcmp-grc.gc.ca'
Subject: Re: CACP video - lawful access

We will consult on this and get back to you shortly.

From: Joe De Mora [mailto:Joe.deMora@rcmp-grc.gc.ca]
Sent: Monday, October 01, 2012 12:56 PM

To: Durand, Stéphanie
Cc: Swift, Andrew; Salewski, Shawn; Christina Cefaloni <Christina.Cefaloni@rcmp-grc.gc.ca>; Joanna Polito <Joanna.Polito@rcmp-grc.gc.ca>; Julie Gagnon <julie.gagnon@rcmp-grc.gc.ca>
Subject: CACP video - lawful access

Stephanie,

Further to our discussions on this subject last week, the RCMP has decided to join the four other invited agencies to participate in a CACP-led video project aimed at providing a police explanation of lawful access. Specifically, it intends to clarify some of the misinformation out there about the tools this initiative would give law enforcement. As you know this is an extremely important topic for the policing community and one that has been met with some vocal public resistance, fueled by a broad misunderstanding and lack of information about what it is and what it isn't. Even if timelines may have shifted in the legislative process, it is important to get the policing side of the story out there along with other very credible partners in law enforcement. In fact, the timing is opportune to inform the public debate now, before the misinformed debate re-ignites and we or the government are faced with having to be on the defensive.

The script of the video is not argumentative but instead focuses on providing facts. It does not confront the government but debunks some of the fallacies that are being communicated by vocal interest groups.

Please find attached the script that we suggest be read by an RCMP spokes as part of the project.

Best

Joe

>>> Joe De Mora 2012-09-25 19:38 >>>
Understood.
-----Original Message-----
From: Durand, Stéphanie<Stephanie.Durand@ps-sp.gc.ca>
Cc: Cefaloni, Christina <Christina.Cefaloni@rcmp-grc.gc.ca>
To: De Mora, Joe <Joe.deMora@rcmp-grc.gc.ca>
Cc: Cox, Greg <Greg.Cox@rcmp-grc.gc.ca>
Cc: Swift, Andrew <Andrew.Swift@ps-sp.gc.ca>
Cc: Salewski, Shawn <Shawn.Salewski@ps-sp.gc.ca>

Sent: 09/25/2012 19:24:54
Subject: Re: More info needed asap on video we discussed

We'll need to discuss tomorrow. Concerns re RCMP participation have been raised.

From: Joe De Mora [mailto:Joe.deMora@rcmp-grc.gc.ca]
Sent: Tuesday, September 25, 2012 04:59 PM
To: Durand, Stéphanie
Cc: Salewski, Shawn; Christina Cefaloni <Christina.Cefaloni@rcmp-grc.gc.ca>; Greg Cox <Greg.Cox@rcmp-grc.gc.ca>
Subject: Re: More info needed asap on video we discussed

CACP led project designed to try to give a police explanation of some of the issues being publicly debated on lawful access.

My understanding is that VPD, as chair of the CACP is leading and have reached out to other CACP partners such as the OPP, Montreal police and others to feature officers reading script that debunks some myths. We are trying to track down what the script we would use is and will share once we have it.

Joe

>>> Durand, Stéphanie<Stephanie.Durand@ps-sp.gc.ca> 2012-09-25 16:53 >>>

Pls advise, thanks.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca<mailto:stephanie.durand@ps-sp.gc.ca>
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada
www.PublicSafety.gc.ca<http://www.publicsafety.gc.ca/> |
www.SecuritePublique.gc.ca<blocked::http://www.securitepublique.gc.ca/>

Durand, Stéphanie

From: Durand, Stéphanie
Sent: Monday, October 01, 2012 5:39 PM
To: 'Joe De Mora'
Subject: RE: CACP video - lawful access

Thanks – did you see my previous note?

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Joe De Mora [mailto:Joe.deMora@rcmp-grc.gc.ca]
Sent: Monday, October 01, 2012 5:35 PM
To: Durand, Stéphanie
Subject: Re: CACP video - lawful access

Steph

As discussed, see the link below that was shared with us as a guideline...

http://youtu.be/MrUu47Lud8k

Joe
>>> Durand, Stéphanie<Stephanie.Durand@ps-sp.gc.ca> 2012-10-01 14:24 >>>
We will consult on this and get back to you shortly.

From: Joe De Mora [mailto:Joe.deMora@rcmp-grc.gc.ca]
Sent: Monday, October 01, 2012 12:56 PM
To: Durand, Stéphanie
Cc: Swift, Andrew; Salewski, Shawn; Christina Cefaloni <Christina.Cefaloni@rcmp-grc.gc.ca>; Joanna Polito <Joanna.Polito@rcmp-grc.gc.ca>; Julie Gagnon <julie.gagnon@rcmp-grc.gc.ca>
Subject: CACP video - lawful access

Stephanie,

Further to our discussions on this subject last week, the RCMP has decided to join the four other invited agencies to participate in a CACP-led video project aimed at providing a police explanation of lawful access. Specifically, it intends to clarify some of the misinformation out there about the tools this initiative would give law enforcement. As you know this is an extremely important topic for the policing community and one that has been met with some vocal public resistance, fueled by a broad misunderstanding and lack of information about what it is and what it isn't. Even if timelines may have shifted in the legislative process, it is important to get the policing side of the story out there along with other very credible partners in law enforcement. In fact, the timing is opportune to inform the public debate now, before the misinformed debate re-ignites and we or the government are faced with having to be on the defensive.

The script of the video is not argumentative but instead focuses on providing facts. It does not confront the government but debunks some of the fallacies that are being communicated by vocal interest groups.

Please find attached the script that we suggest be read by an RCMP spokes as part of the project.

Best

Joe

>>> Joe De Mora 2012-09-25 19:38 >>>
Understood.
-----Original Message-----
From: Durand, Stéphanie<Stephanie.Durand@ps-sp.gc.ca>
Cc: Cefaloni, Christina <Christina.Cefaloni@rcmp-grc.gc.ca>
To: De Mora, Joe <Joe.deMora@rcmp-grc.gc.ca>
Cc: Cox, Greg <Greg.Cox@rcmp-grc.gc.ca>
Cc: Swift, Andrew <Andrew.Swift@ps-sp.gc.ca>
Cc: Salewski, Shawn <Shawn.Salewski@ps-sp.gc.ca>

Sent: 09/25/2012 19:24:54
Subject: Re: More info needed asap on video we discussed

We'll need to discuss tomorrow. Concerns re RCMP participation have been raised.

From: Joe De Mora [mailto:Joe.deMora@rcmp-grc.gc.ca]
Sent: Tuesday, September 25, 2012 04:59 PM
To: Durand, Stéphanie
Cc: Salewski, Shawn; Christina Cefaloni <Christina.Cefaloni@rcmp-grc.gc.ca>; Greg Cox <Greg.Cox@rcmp-grc.gc.ca>
Subject: Re: More info needed asap on video we discussed

CACP led project designed to try to give a police explanation of some of the issues being publicly debated on lawful access.

My understanding is that VPD, as chair of the CACP is leading and have reached out to other CACP partners such as the OPP, Montreal police and others to feature officers reading script that debunks some myths. We are trying to track down what the script we would use is and will share once we have it.

Joe

>>> Durand, Stéphanie<Stephanie.Durand@ps-sp.gc.ca> 2012-09-25 16:53 >>>
Pls advise, thanks.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca<mailto:stephanie.durand@ps-sp.gc.ca>
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada
www.PublicSafety.gc.ca<http://www.publicsafety.gc.ca/> |
www.SecuritePublique.gc.ca<blocked::http://www.securitepublique.gc.ca/>

Durand, Stéphanie

From: Durand, Stéphanie
Sent: Monday, October 01, 2012 5:32 PM
To: Carmichael, Julie; McGrath, Andrew
Cc: Swift, Andrew; Carta, John; Manji, Natasha; Binnie, Kate; Salewski, Shawn
Subject: Re: CACP video - lawful access

Thanks - I'll concey to the RCMP (again).

From: Carmichael, Julie
Sent: Monday, October 01, 2012 03:40 PM
To: Durand, Stéphanie; McGrath, Andrew
Cc: Swift, Andrew; Carta, John; Manji, Natasha; Binnie, Kate; Salewski, Shawn
Subject: Re: CACP video - lawful access

Not approved

Julie Carmichael
Director of Communications
Office of the Minister of Public Safety
Julie.carmichael@ps-sp.gc.ca

From: Durand, Stéphanie
Sent: Monday, October 01, 2012 03:26 PM
To: Carmichael, Julie; McGrath, Andrew
Cc: Swift, Andrew; Carta, John; Manji, Natasha; Binnie, Kate; Salewski, Shawn
Subject: FW: CACP video - lawful access

See below. Further to our chat last week on this. VPD, as chair of the CACP is leading and have reached out to other CACP partners such as the OPP, Montreal police and others to feature officers reading script that debunks some myths. The video is designed to try to give a police explanation of some of the issues being publicly debated on lawful access.

RCMP would still like to proceed and take part in the video. Attached is the script they would use. RCMP understands that this would likely not be approved. Please advise.
I am trying to get a copy of the overall script for the video. RCMP is following-up on this to give you more context....

Thanks.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Joe De Mora [mailto:Joe.deMora@rcmp-grc.gc.ca]
Sent: Monday, October 01, 2012 12:56 PM
To: Durand, Stéphanie
Cc: Swift, Andrew; Salewski, Shawn; Christina Cefaloni; Joanna Polito; Julie Gagnon
Subject: CACP video - lawful access
Stephanie,

Further to our discussions on this subject last week, the RCMP has decided to join the four other invited agencies to participate in a CACP-led video project aimed at providing a police explanation of lawful access. Specifically, it intends to clarify some of the misinformation out there about the tools this initiative would give law enforcement. As you know this is an extremely important topic for the policing community and one that has been met with some vocal public resistance, fueled by a broad misunderstanding and lack of information about what it is and what it isn't. Even if timelines may have shifted in the legislative process, it is important to get the policing side of the story out there along with other very credible partners in law enforcement. In fact, the timing is opportune to inform the public debate now, before the misinformed debate re-ignites and we or the government are faced with having to be on the defensive.

The script of the video is not argumentative but instead focuses on providing facts. It does not confront the government but debunks some of the fallacies that are being communicated by vocal interest groups.

Please find attached the script that we suggest be read by an RCMP spokes as part of the project.

Best

Joe

CACP video version 2 – Lawful access clip 3

"Right now police can call up any telecommunications company and ask for basic subscriber information without ever having to prove the request is lawfully legitimate." ...TRUE

"That is correct, but that all changes with new lawful access legislation – and police applaud that. It's going to put accountability where accountability needs to be. It will give Canadians comfort and confidence. So what are these changes? Well, instead of any police officer being able to contact a telecommunications company and request basic subscriber information, only a few "designated" officers will be able to do that. All of the requests will be in writing, and will have to be kept on file for review and audit by the Privacy Commissioner or other public bodies."

Durand, Stéphanie

From: Durand, Stéphanie
Sent: Monday, October 01, 2012 2:24 PM
To: 'Joe.deMora@rcmp-grc.gc.ca'
Cc: Swift, Andrew; Salewski, Shawn; 'Christina.Cefaloni@rcmp-grc.gc.ca'; 'joanna.polito@rcmp-grc.gc.ca'; 'julie.gagnon@rcmp-grc.gc.ca'; 'Daniel.Lavoie@rcmp-grc.gc.ca'
Subject: Re: CACP video - lawful access

We will consult on this and get back to you shortly.

From: Joe De Mora [mailto:Joe.deMora@rcmp-grc.gc.ca]
Sent: Monday, October 01, 2012 12:56 PM
To: Durand, Stéphanie
Cc: Swift, Andrew; Salewski, Shawn; Christina Cefaloni <Christina.Cefaloni@rcmp-grc.gc.ca>; Joanna Polito <Joanna.Polito@rcmp-grc.gc.ca>; Julie Gagnon <julie.gagnon@rcmp-grc.gc.ca>
Subject: CACP video - lawful access

Stephanie,

Further to our discussions on this subject last week, the RCMP has decided to join the four other invited agencies to participate in a CACP-led video project aimed at providing a police explanation of lawful access. Specifically, it intends to clarify some of the misinformation out there about the tools this initiative would give law enforcement. As you know this is an extremely important topic for the policing community and one that has been met with some vocal public resistance, fueled by a broad misunderstanding and lack of information about what it is and what it isn't. Even if timelines may have shifted in the legislative process, it is important to get the policing side of the story out there along with other very credible partners in law enforcement. In fact, the timing is opportune to inform the public debate now, before the misinformed debate re-ignites and we or the government are faced with having to be on the defensive.

The script of the video is not argumentative but instead focuses on providing facts. It does not confront the government but debunks some of the fallacies that are being communicated by vocal interest groups.

Please find attached the script that we suggest be read by an RCMP spokes as part of the project.

Best

Joe

>>> Joe De Mora 2012-09-25 19:38 >>>
Understood.
-----Original Message-----
From: Durand, Stéphanie<Stephanie.Durand@ps-sp.gc.ca>
Cc: Cefaloni, Christina <Christina.Cefaloni@rcmp-grc.gc.ca>
To: De Mora, Joe <Joe.deMora@rcmp-grc.gc.ca>
Cc: Cox, Greg <Greg.Cox@rcmp-grc.gc.ca>
Cc: Swift, Andrew <Andrew.Swift@ps-sp.gc.ca>
Cc: Salewski, Shawn <Shawn.Salewski@ps-sp.gc.ca>

Sent: 09/25/2012 19:24:54
Subject: Re: More info needed asap on video we discussed

We'll need to discuss tomorrow. Concerns re RCMP participation have been raised.

From: Joe De Mora [mailto:Joe.deMora@rcmp-grc.gc.ca]
Sent: Tuesday, September 25, 2012 04:59 PM
To: Durand, Stéphanie
Cc: Salewski, Shawn; Christina Cefaloni <Christina.Cefaloni@rcmp-grc.gc.ca>; Greg Cox <Greg.Cox@rcmp-grc.gc.ca>
Subject: Re: More info needed asap on video we discussed

CACP led project designed to try to give a police explanation of some of the issues being publicly debated on lawful access.

My understanding is that VPD, as chair of the CACP is leading and have reached out to other CACP partners such as the OPP, Montreal police and others to feature officers reading script that debunks some myths. We are trying to track down what the script we would use is and will share once we have it.

Joe

>>> Durand, Stéphanie<Stephanie.Durand@ps-sp.gc.ca> 2012-09-25 16:53 >>>
Pls advise, thanks.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca<mailto:stephanie.durand@ps-sp.gc.ca>
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada
www.PublicSafety.gc.ca<http://www.publicsafety.gc.ca/> |
www.SecuritePublique.gc.ca<blocked::http://www.securitepublique.gc.ca/>

Paulson, Erika

From: Wilson, Barbara
Sent: Thursday, September 27, 2012 10:30 AM
To: Paulson, Erika
Subject: FW: NEW Petition 411-1784 - Lawful Access
Attachments: 411-1519 - Signed response.pdf; 411-1784-notice.doc; 411-1784 petition response.doc

Importance: High

For info Erika. In case you're interested.

Barbara Wilson
Senior Communications Advisor
Issues management and media relations
Conseillère principale en communications
Gestion des enjeux et relations avec les médias
Public Safety Canada/Sécurité publique Canada
269 Laurier Avenue W/ 269, avenue Laurier ouest
Ottawa, (ON) K1P 0P8
(613) 944-4920
barbara.wilson@ps-sp.gc.ca

From: Issues / Enjeux
Sent: Thursday, September 27, 2012 10:11 AM
To: McDonald, Jessica; Picard, Josée; Swift, Andrew; Filipps, Lisa; Manning, Kerri; Champoux, Martin; Wilson, Barbara; Slack, Jessica; Miller, Kevin; Duval, Jean Paul; Van Criekingen, Jane; Taillefer, Lucie
Subject: FW: NEW Petition 411-1784 - Lawful Access
Importance: High

From: Leclair, Natalie
Sent: Thursday, September 27, 2012 10:11:02 AM (UTC-05:00) Eastern Time (US & Canada)
To: Dupuis, Chantal; Bedor, Tia Leigh; Baulne, Lucie
Cc: McAteer, Julie; Issues / Enjeux; Chang, Anna
Subject: NEW Petition 411-1784 - Lawful Access

Good afternoon,

Please find attached a new petition 411-1784 which was presented in the House by Ms. May concerning Telecommunications.

Please note that this petition is similar to previous petitions on this subject. (previous petition 411-1519 attached).

NOTE: Please ensure that the information provided in the response to the petition is accurate and consistent with information or documents already disclosed under the *Access to Information Act* or the *Privacy Act*, or in response to other types of information requests.

Your ADM/ADM equivalent approved bilingual response should sent electronically to me with a CC to Julie McAteer **by COB on October 9, 2012**.

Please do not hesitate to contact me should you have any questions.

Thank you.
Nat

Natalie Leclair
Advisor / Conseillère
Parliamentary Affairs / Affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 990-2718
Fax: (613) 954-8774
Email/Courriel: natalie.leclair@ps-sp.gc.ca

PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

PETITION NO./Nº DE LA PÉTITION	BY / DE	DATE
411-1519	Ms. Savoie (Victoria)	June 21, 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 has introduced the *Protecting Children from Internet Predators Act.*

We want to fix our laws while striking the right balance when it comes to protecting privacy.

Bill C-30 creates no new powers to access the content of e-mails or phone calls beyond that which already exists in Canadian law.

We will send this legislation directly to Committee for a full examination of potential amendments to achieve the best protection for our children.

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.

.../2

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.

PETITION NO./Nº DE LA PÉTITION	BY / DE	DATE
411-1519	Mme. Savoie (Victoria)	21 juin 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 la *Loi sur la protection des enfants contre les cyberprédateurs*.

Nous voulons modifier nos lois tout en établissant un juste équilibre avec la protection de la vie privée.

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.

Nous enverrons ce projet de loi directement au comité pour un examen complet d'amendements potentiels afin d'atteindre la meilleure protection pour nos enfants.

...12

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) à 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 demandes 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.

.../3

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.

Government of Canada
Privy Council Office

Gouvernement du Canada
Bureau du Conseil privé

PETITION - PÉTITION

To / À **PUBLIC SAFETY**

Date **September 27, 2012**

SUBJECT: Petition No. / Pétition N° **411-1784**

SUJET: Member / Député **MS. MAY (SAANICH-GULF ISLANDS)**

Date of Petition / Date de la pétition **September 24, 2012**

FOR PRIORITY ATTENTION

Section 36 (8) of the Standing Orders:

(a) Every petition presented pursuant to this Standing Order shall forthwith be transmitted to the Ministry, which shall, within forty-five days, respond to every petition referred to it; provided that the said response may be tabled pursuant to S.O. 32(1).

(b) If such a petition remains without a response at the expiration of the said period of forty-five days, the matter of the failure of the Ministry to respond shall be deemed referred to the appropriate Standing Committee. Within five sitting days of such a referral the Chair of the committee shall convene a meeting of the committee to consider the matter of the failure of the Ministry to respond.

Would you please respond to this petition before

November 2, 2012

The response should be prepared on a "Response to Petition" form in both official languages.

If you have no information on this subject or you consider that another department should be contacted, please advise us without delay.

POUR EXAMEN PRIORITAIRE

Paragraphe 36 (8) du Règlement:

a) Toute pétition présentée conformément au présent article est transmise sur-le-champ au gouvernement, qui répond dans les quarante-cinq jours à toutes les pétitions qui lui sont renvoyées. La réponse peut être déposée conformément à l'article 32(1) du Règlement.

b) Dans le cas où une pétition reste sans réponse à l'expiration de ce délai de quarante-cinq jours, cette absence de réponse de la part du gouvernement est réputée renvoyée au comité permanent concerné. Dans les cinq jours de séance suivants ce renvoi, le président du comité convoque une réunion pour se pencher sur l'absence de réponse de la part du gouvernement.

Veuillez répondre à cette pétition avant le

La réponse doit être présentée dans les deux langues officielles sur le formulaire "Réponse à la pétition".

Si vous ne possédez aucun renseignement sur ce sujet ou si vous jugez qu'un autre ministère devrait être contacté, veuillez nous aviser sans délai.

Nicole Baker

Nicole Baker
Coordinator of Parliamentary Returns
Coordonnatrice des documents parlementaires

Canada

ASSIGNMENT: **PUBLIC SAFETY**
ASSIGNATION:

SUBJECT/SUJET

— by Ms. May (Saanich—Gulf Islands), one concerning **environmental assessment and review** (No. 411-1783) and one concerning **telecommunications** (No. 411-1784).	— par M^me^ May (Saanich—Gulf Islands), une au sujet de **l'examen et des évaluations environnementales** (n° 411-1783) et une au sujet au sujet des **télécommunications** (n° 411-1784).

REPEAT OF / RÉPÉTITION DE LA : 411-1519

NOTE:

The subject to be typed on the form Response to Petition should be the same as the one in the Journals. (See Subject/Sujet above)

Le sujet à dactylographier sur le formulaire Réponse à la Pétition doit être le même que celui des Journaux. (Voir Subject/Sujet ci-haut)

Canada

411-1784

PETITION TO THE HOUSE OF COMMONS

We, the undersigned residents of Canada, draw the attention of the House of Commons to the following:

THAT Canadians do not wish to allow warrantless surveillance by a range of government authorities, including access to financial and personal information, through internet and mobile devices.

THAT Federal and Provincial/Territorial Commissioners to Privacy have voiced concern that Bill C-30 will allow unacceptable intrusions into privacy rights.

THAT requiring internet and service providers to provide the information to authorities will lead to costs that will be passed on to the purchaser of the internet and mobile services, rather than borne by the authorities requesting the information.

THAT Canadians do not need a level of surveillance that is typically associated with totalitarian regimes.

THAT Canadians need privacy protection that reflects the present state of communication technology and the rights and freedoms they enjoy under the Constitution.

THEREFORE, your petitioners call upon the Government of Canada to reject those aspects of the proposed lawful access that expand surveillance, allow authorities unrestricted and warrantless access to personal information and violate the privacy of Canadians. Bill C-30 must be amended sufficiently that it is supported by federal and provincial/territorial privacy commissioners.

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

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

Willey, Chris

From: Paulson, Erika
Sent: Tuesday, September 18, 2012 7:17 AM
To: Austria, Jamela; Willey, Chris
Subject: FYI: Understanding the Lawful Access Decryption Requirement | Technology, Thoughts, and Trinkets

FYI - you may want to flag this to policy. Chris Parsons has written a paper on LA decryption.

http://www.christopher-parsons.com/blog/privacy/understanding-the-lawful-access-decryption-requirement/

Understanding the Lawful Access Decryption Requirement Posted on September 17, 2012 by Christopher

For several months I and a handful of others in the Canadian privacy and security community have been mulling over what Bill C-30, better known as Canada's 'lawful access' legislation, might mean for the future of encryption policy in Canada. Today, I'm happy to announce that one of the fruits of these conversation, a paper that I've been working on with Kevin McArthur, is now public. The paper, titled "Understanding the Lawful Access Decryption Requirement," spends a considerable amount of time considering the potential implications of the legislation. Our analysis considers how C-30 might force companies to adopt key escrows, or decryption key repositories. After identifying some of the problems associated with these repositories, we suggest how to amend the legislation to ensure that corporations will not have to establish key escrows. We conclude by outlining the dangers of leaving the legislative language as it stands today. The full abstract, and download link, follows.

Abstract

Canada's lawful access legislation, Bill C-30, includes a section that imposes decryption requirements on telecommunications service providers. In this paper we analyze these requirements to conclude that they may force service providers to establish key escrow, or decryption key retention, programs. We demonstrate the significance of these requirements by analyzing the implications that such programs could have for online service providers, companies that provide client software to access cloud services, and the subscribers of such online services. The paper concludes by suggesting an amendment to the bill, to ensure that corporations will not have to establish escrows, and by speaking to the dangers of not implementing such an amendment.

Erika Paulson
Tel: 613-993-4415 | BB: [redacted] s.19(1)

Wilson, Barbara

From: Miller, Kevin
Sent: Thursday, August 30, 2012 2:55 PM
To: Duval, Jean Paul; Wilson, Barbara; Slack, Jessica
Cc: Champoux, Martin
Subject: FW: Notification - Globe & Mail - C-30 Lawful Access

FYI

From: Carmichael, Julie
Sent: Thursday, August 30, 2012 1:05 PM
To: Durand, Stéphanie
Cc: Miller, Kevin
Subject: RE: Notification - Globe & Mail - C-30 Lawful Access

Bill C-30 will be sent to committee for major review before proceeding further. Minister Toews was very clear on February 15th regarding this matter. Decisions on timing of Bills and Parliamentary strategy are made by the Government House Leader, in consultation with the relevant Ministers

From: Durand, Stéphanie
Sent: August-30-12 12:56 PM
To: Carmichael, Julie
Cc: Miller, Kevin
Subject: RE: Notification - Globe & Mail - C-30 Lawful Access

Can you share your response pls?
Thanks.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Carmichael, Julie
Sent: Thursday, August 30, 2012 11:12 AM
To: Duval, Jean Paul; McGrath, Andrew; Johnson, Mark; Thibouthot, AkimIsabelle; Williams, Christpher
Cc: Champoux, Martin; Durand, Stéphanie; Swift, Andrew; Slack, Jessica
Subject: RE: Notification - Globe & Mail - C-30 Lawful Access

I'll take it

From: Duval, Jean Paul
Sent: August-30-12 10:39 AM
To: Carmichael, Julie; McGrath, Andrew; Johnson, Mark; Thibouthot, AkimIsabelle; Williams, Christpher
Cc: Champoux, Martin; Durand, Stéphanie; Swift, Andrew; Slack, Jessica
Subject: Notification - Globe & Mail - C-30 Lawful Access

Hi Julie,

We received a request from the Globe and Mail on Lawful Access Bill C-30.

Did you want to take this call? s.19(1)

Regards,
JP

Reporter's Name	[redacted]
Media Outlet	Globe and Mail
Call Date	8/30/2012 11:00 AM
Telephone	[redacted](cell)
E-mail address	[redacted]@globeandmail.com
Deadline	8/30/2012 5:00 PM
Status	Consulting
Branch	
Subject	Lawful Access Bill
Questions	Hello, A couple of questions on Bill C-30, tabled in February of this year: On what date was the decision made to send the bill straight to committee? Who decided? When were public servants and policy advisors working on the bill told of the change? Is this normal procedure? On what date did the Minister's office receive a full clause-by-clause analysis of the bill? If possible to get answers by end of day today, that would be fantastic. Please let me know how things look on your end.

Jean Paul Duval
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-1689
Cell | Portable: [redacted]
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

Durand, Stéphanie

From: Durand, Stéphanie
Sent: Thursday, August 30, 2012 1:12 PM
To: Carmichael, Julie
Subject: RE: Notification - Globe & Mail - C-30 Lawful Access

thx

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

From: Carmichael, Julie
Sent: Thursday, August 30, 2012 1:05 PM
To: Durand, Stéphanie
Cc: Miller, Kevin
Subject: RE: Notification - Globe & Mail - C-30 Lawful Access

Bill C-30 will be sent to committee for major review before proceeding further. Minister Toews was very clear on February 15th regarding this matter. Decisions on timing of Bills and Parliamentary strategy are made by the Government House Leader, in consultation with the relevant Ministers

From: Durand, Stéphanie
Sent: August-30-12 12:56 PM
To: Carmichael, Julie
Cc: Miller, Kevin
Subject: RE: Notification - Globe & Mail - C-30 Lawful Access

Can you share your response pls?
Thanks.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada

From: Carmichael, Julie
Sent: Thursday, August 30, 2012 11:12 AM
To: Duval, Jean Paul; McGrath, Andrew; Johnson, Mark; Thibouthot, AkimIsabelle; Williams, Christpher
Cc: Champoux, Martin; Durand, Stéphanie; Swift, Andrew; Slack, Jessica
Subject: RE: Notification - Globe & Mail - C-30 Lawful Access

I'll take it

From: Duval, Jean Paul
Sent: August-30-12 10:39 AM
To: Carmichael, Julie; McGrath, Andrew; Johnson, Mark; Thibouthot, AkimIsabelle; Williams, Christpher
Cc: Champoux, Martin; Durand, Stéphanie; Swift, Andrew; Slack, Jessica
Subject: Notification - Globe & Mail - C-30 Lawful Access

Hi Julie,

We received a request from the Globe and Mail on Lawful Access Bill C-30.

Did you want to take this call?

Regards,
JP

Reporter's Name	[redacted]
Media Outlet	Globe and Mail
Call Date	8/30/2012 11:00 AM
Telephone	[redacted] (cell)
E-mail address	[redacted]@globeandmail.com
Deadline	8/30/2012 5:00 PM
Status	Consulting
Branch	
Subject	Lawful Access Bill
Questions	Hello, A couple of questions on Bill C-30, tabled in February of this year: On what date was the decision made to send the bill straight to committee? Who decided? When were public servants and policy advisors working on the bill told of the change? Is this normal procedure? On what date did the Minister's office receive a full clause-by-clause analysis of the bill? If possible to get answers by end of day today, that would be fantastic. Please let me know how things look on your end.

s.19(1)

Jean Paul Duval
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-991-1689

Cell | Portable: [redacted]
Email | Courriel : jeanpaul.duval@ps-sp.gc.ca

s.19(1)

Willey, Chris

From: Carta, John
Sent: Tuesday, August 14, 2012 12:46 PM
To: Willey, Chris; Austria, Jamela
Subject: FW: lawful access article

fyi

From: Burton, Meredith
Sent: August-14-12 12:24 PM
To: Carta, John; Miller, Kevin
Subject: lawful access article

Article of note.

http://www.slate.com/articles/technology/future_tense/2012/08/how_governments_and_telecom_companies_work_together_on_surveillance_laws_.html

Manager, Regional Communications / Gestionnaire, Communications régionales
Public Safety Canada / Sécurité Publique Canada
Tel: 613-949-6583
Cel: s.19(1)
Fax: 613-993-7062
meredith.burton@ps-sp.gc.ca