Public Safety Canada | Sécurité publique Canada

Deputy Minister | Sous-ministre

Ottawa, Canada
K1A 0P8

T.D No / No. D.T.	346838
Routed to / Envoyé à	MIN
CC	NAA, SAA, CMB, LGS
B.F / A.R	DMO, ECI
File No / No Dossier	6000-7

SECRET

DATE: JUL 11 2007

6950-1/346838

MEMORANDUM FOR THE MINISTER

PROPOSED CONSULTATION STRATEGY ON ACCESS TO CUSTOMER NAME AND ADDRESS INFORMATION

(For Decision)

ISSUE

- Law enforcement and CSIS officials often require quick access to basic contact information (customer name, address, telephone number, e-mail/Internet Protocol address) for telephone and Internet service customers. This information may be publicly available but officials require the most accurate information, quickly, which is best obtained directly from the telephone or Internet provider.

- As a result of deregulation of the telecommunications sector there are hundreds of companies providing telephone and Internet services. When police request basic contact information on customers, some companies provide it while others refuse. This compels police to seek a court order to compel disclosure.

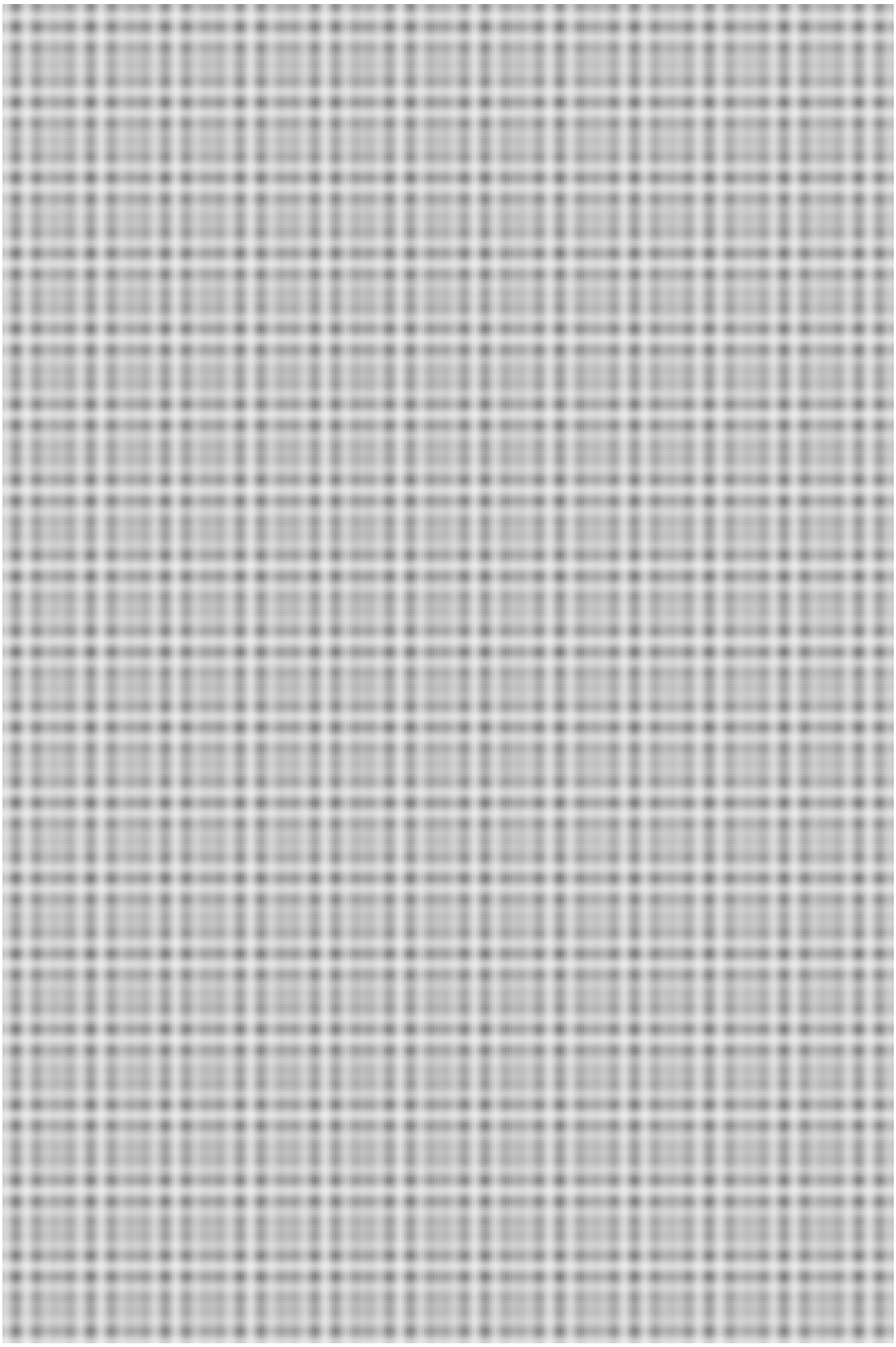
Not relevant

[redacted]

Canada

SECRET

Not relevant



Not relevant

[redacted]

Past Consultations

- Numerous organizations and individuals were consulted during the 2002 and 2005 consultations on lawful access. **TAB B** contains a list of those organizations and individuals.

- Stakeholder views on the subscriber information proposals were varied. Law enforcement stakeholders provided examples of how uncertainty in the law has resulted in delays to important investigations. Privacy advocates expressed concern with any proposal that may infringe on the privacy rights of Canadians. Industry stakeholders were primarily concerned with the details of the proposals, such as the timeframe in which they would have to provide the information and whether they would be compensated. **TAB C** contains an overview of the views expressed in consultations as they relate to the customer name and address proposal.

Proposed New Consultations

- There are several issues that should be considered with respect to additional consultations, namely: stakeholder composition; the proposed content; and the location, timing and format.

Stakeholders:

- The lawful access initiative brings together a diverse group of stakeholders with sometimes competing interests. For example, the police have lobbied for prompt action to maintain their investigative capabilities, while industry has pressured government officials to ensure that the proposals will not restrict the growth and evolution of communications technology. Human rights advocates have consistently expressed concern that government action not erode or infringe upon personal privacy or other human rights.

- Given this diverse range of stakeholders, it is recommended that the consultation be reflective of these groups. A proposed list of stakeholders is contained in **TAB D**, and represents members of the telecommunications industry, consumer and privacy advocates, and law enforcement. The list also contains names of individuals and organizations that were supplied by officials in your Office.

What:

- Considerable work has taken place in the development of the administrative model for accessing customer name and address information. The TALEA proposals were informed by the previous consultations, and represent a balancing of the needs of law enforcement, industry and privacy groups. It is recommended that the proposed consultation focus on this administrative model and seek to reaffirm stakeholders' views on this model.

Where:

- It is recommended that the consultation occur in Ottawa. Transportation costs for those coming from outside of Ottawa will be borne by the individual participants.

Timing:

- Officials were asked to undertake a summer consultation, however, given the difficulty in securing adequate participation during this period, and due to the fact that a summer consultation may be viewed by some as minimizing the importance of this issue, it is recommended that the consultation be held in early to mid-September. **Not relevant**

Type:

- Regarding the format of the proposed consultation, a roundtable style meeting is recommended. The meeting would begin with stakeholders being briefed by government officials on the proposal, and then feedback from the stakeholders would be solicited during subsequent roundtable discussion.

CONSIDERATIONS

- A third round of consultations on the customer name and address proposals will confirm the government's commitment to an informed and balanced approach. It will also signal that all relevant views are being considered and that a balance will be struck among divergent perspectives. At the same time, the need for consultations may be questioned by some participants, since proposals will be substantially the same as in past consultations.

- It is anticipated that law enforcement stakeholders who have in the past objected to the slow pace of this initiative will likely raise concerns that the

government is not proceeding quickly enough with legislation. As they have done in the past, privacy advocates will likely criticize the government for considering proposals that they view as eroding Canadians' privacy. Industry stakeholders will likely be cautious and express an understanding for the need for this information by the police. However, some may voice concerns over the privacy rights of their customers, particularly when questioned by the media.

- Another consultation will also likely raise the profile of this issue. It is anticipated that there would be media articles and strong negative reactions from some more entrenched stakeholders/advocates who oppose both the customer name and address proposals and the interception capability element of the package.

Not relevant

- [redacted]

RECOMMENDATION

- It is recommended that we proceed as proposed.

Suzanne Hurtubise

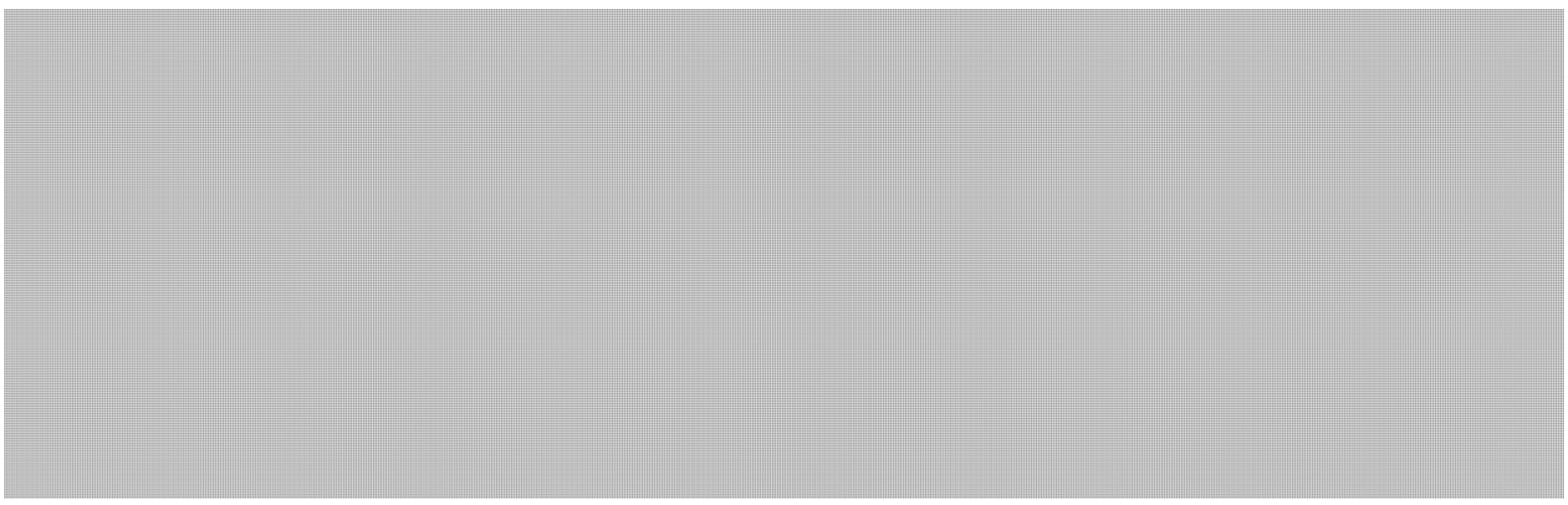
Enclosures: (4)

TAB A

Access to Customer Name and Address Information
- International Comparison -

Not relevant

Canada – *TALEA* proposals



United States

In the U.S., this information can be obtained by a Grand Jury Subpoena in a criminal investigation. The subpoena is issued by the court clerk's office, completed by the prosecuting attorney, and served on the company, usually by a police officer or federal marshal. This is also used to obtain much more than just subscriber information – subscriber information such as name and address is often available to U.S. law enforcement through public source information. In the

context of a national security investigation, U.S. law enforcement obtains this information pursuant to a national security letter, authorized under the *Patriot Act*.

Australia

Not relevant

In Australia, there is a legislative scheme for such access, set out in the *Telecommunications Act 1997*. Under the Act, a law enforcement agency can request subscriber information from a service provider where the disclosure of that information is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty or the protection of the public revenue. The Australian Security Intelligence Organization (ASIO) can request the disclosure of subscriber information where the disclosure is connected with the performance of its functions. The request will be made by an authorized officer of a law enforcement agency (usually Inspector or above) or an authorized employee of ASIO. These authorizations must be issued in writing by the head of the relevant agency. Records of these disclosures must be kept by the service providers for three years, and there are annual reports on the number of disclosures, broken down by reason of request, as part of the annual report prepared by the industry regulator. There are no specific oversight or review mechanisms for this access.

United Kingdom

Not relevant

In the United Kingdom, there is a legislative scheme for such access, set out in the *Regulation of Investigatory Powers Act 2000 (RIPA)*.

Under RIPA, Part 1, Chapter II, there are provisions for access to all types of communications data, including subscriber data. RIPA sets out how public authorities can be granted access to data (it lists some public authorities in its schedules and more have been added over time by means of orders approved by Parliament), who can authorize access (internal authorization of designated persons at various specified levels of seniority depending on the type of data to be accessed), specific purposes for which data can be acquired and how data is acquired (two methods: a notice served on a TSP or an authorization which permits online access to this information). There is also provision for a statutory code of practice to be created – a draft of this was recently provided to Parliament for approval. There are provisions for oversight – access is overseen by the Interception of Communications Commissioner, as provided for by Part IV of RIPA. The Commissioner reports annually to the Prime Minister and the unclassified portion of this report is published in Parliament – it contains, for example, information on numbers of requests.

TAB A

Ireland

Not relevant

In Ireland, there is a legislative scheme for such access, [redacted] although perhaps what was proposed by the Parliamentary Committee for *PIPEDA* would be a closer parallel, as Irish authorities access this information under their Data Protection Acts, 1988-2003. This legislation provides that restrictions on disclosure of personal data do not apply if, *inter alia*, the disclosure is:

- in the opinion of a member of the Garda Síochána [national police service] not below the rank of chief superintendent or any officer of the Permanent Defence Force who holds an army rank not below that of colonel and is designated by the Minister for Defence, required for the purpose of safeguarding the security of the State;
- required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State;
- required in the interests of protecting the international relations of the State;
- required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property; and
- required by or under any enactment or by a rule of law or order of a court.

Only the Garda Síochána [national police service, which also acts as the State's internal security service] and the Permanent Defence Force may obtain subscriber information. In the case of the Garda Síochána, only officers at chief superintendent rank or above may make requests for subscriber information and, in the case of the Permanent Defence Force, only officers at colonel rank or above may make such requests. A record of each request is prepared. There are no specific oversight or review mechanisms. Subscriber information may be obtained in the interests of national security and for the purpose of preventing, detecting or investigating any offence. There is no public report in relation to the number of nature of these requests.

TAB B
- Previous Consultation Stakeholders -

List of Stakeholders That Responded to the 2002 Public Consultation Document

Industry

ITAC
IBM Canada
Motorola Canada
Rogers Cable
Bell Canada
AT&T Canada
Telus
Call-Net
Microcell
Shaw
Cogeco
Rogers Wireless Inc.
Bell Mobility
Telus Mobility
AOL
Microcell
Ontario Tel. Ass.
Vidéotron Télécommunications
Zero-Knowledge Systems Inc.
SecureOps Inc.
SipherShare Systems Inc.
Entrust Inc.
ABT Advanced Biometric Techno
AEPOS Technologies Corporation
CAIP
CWTA
EWA Canada
CRIM
CCTA
MTS
CATA
Mouvement Desjardins
Transcontinental Medias
Telecommunications Workers Union
Privaterra
Prolesta
Digital Discretion
EWA-IIT
Spyrus
Cottingham Group
Fites & Associates
E-commerce Market Development

Privacy Advocates

Privacy Commissioner of Canada
Osler, Hoskin and Harcourt
Office of the Privacy Commission
Davies Ward Phillips & Vineberg
DataPrivacy Partners Ltd.
Computer Professionals for Social Responsibility
University of Ottawa, Faculty of Law
Civil Liberties – NCR
Queen's University
Information and Privacy Commission of Ontario
University of Toronto/CPSR
Public Interest Advocacy Centre
Carrefour mondial de l'internet citoyen
Ligue des droits et libertés
Barreau du Québec
Option Consommateurs
Direction informatique
Institut du commerce électronique
Association des étudiants en droit de l'UQAM
Commission d'accès à l'information
Association étudiante - science politique et droit - UQUAM
Commission d'accès à l'information
Collège des médecins du Québec
Ligue des droits et libertés
BC Civil Liberties Association
BC Institute of Technology
BC Freedom of Information and Privacy Association
British Columbia Civil Liberties Association
Telecom Consultant
Committee for Racial Justice
Margo Langford, Barrister & Solicitor,
New Media Specialist
SFU School of Communications

TAB B
- Previous Consultation Stakeholders -

Canadian Bar Association
Corporate Privacy and Information Access Branch, Gov. of BC

Privacy Prime Consulting
Digital Discretion
Manitoba Association for Rights and Liberties

Law Enforcement

Abbotsford Police Department
Barrie Police Service
Brantford Police Service
Brockville Police Service
Calgary Police Service
Canadian Association of Chiefs of Police
Charlottetown Police Department
Chatham-Kent Police Service
CN Police
Criminal Intelligence Service Alberta
Département de police de la ville de Laval
Durham Regional Police Service
Edmonton Police Service
Greater Sudbury Police Service
Guelph Police Service
Halton Regional Police Service
Hamilton Police Service
Lethbridge Police Service
London Police Service
New Liskeard Police Service
Niagara Regional Police Service
Oak Bay Police Department
Ontario Provincial Police
Ottawa Police Service
Oxford Community Police
Peterborough Lakefield Community Police Service
RCMP – Calgary
RCMP - Edmonton
RCMP – Halifax
RCMP – Kelowna
RCMP – London
RCMP – Montreal
RCMP – New Brunswick
RCMP – Ottawa
RCMP – Prince Edward Island
RCMP – Quebec City
RCMP – Red Deer
RCMP – Strathcona County Detachment
RCMP – Toronto
RCMP – Vancouver
RCMP – Whitehorse
Régie intermunicipale de police – Vallée du Richelieu
Regina Police Service
Royal Newfoundland Constabulary
Saint John Police Force
Saskatoon Police Service
Sault Ste. Marie Police Service
Sûreté municipale de Mont-Tremblant
Thunder Bay Police
Timmins Police Service
Toronto Police Service
Truro Police Service
Vancouver Police Department
Waterloo Regional Police Service
Weyburn Police Service
Winnipeg Police Service

Other

Department of Computer Science (University of British Columbia)
Vancouver Community Network
Government of Alberta Innovation and Science
Camosun College
Simon Fraser University Library
Faculty of Commerce – University of British Columbia
Government of Ontario

TAB B
- Previous Consultation Stakeholders -
2005 List of Stakeholders That Participated In The In-Depth Follow-up Consultations

Industry

Information Technology Association of Canada (ITAC)
Canadian Wireless Telecommunications Association (CWTA)
Canadian Cable Telecommunications Association (CCTA)
Canadian Advanced Technology Alliance (CATA)
Bell Canada
Bell Mobility
TELUS
Telemobile
Rogers Communications
Rogers Wireless
Quebecor/Videotron
MTS Allstream
Cogeco
Supernet
Mobile Satellite Ventures
Telesat
Yahoo
Shaw

Vendors/Manufactures/Solution Providers

Cisco
TopLayer
SS8
ETI Connect
Motorola
Lucent
Verint
Ericsson
Spectronic
Juniper
Siemens
Aqsacom
Detica
Nortel

Law Enforcement

CACP Law Amendments Committee (LAC)
CACP Lawfully Authorized Electronic Surveillance (LAES) Sub-group
RCMP Special I

TAB C

PREVIOUS CONSULTATIONS ON LAWFUL ACCESS - CUSTOMER NAME AND ADDRESS PROPOSALS -

BACKGROUND

- The issue of lawful access has been the subject of two rounds of consultations in 2002 and 2005. Additional discussions were held with select industry representatives and police organizations in 2006 and 2007.

2002 Consultations

- In the fall of 2002, representatives from the former Solicitor General's Department, Justice Canada, Industry Canada, the Competition Bureau, the RCMP and CSIS undertook consultations on lawful access. These officials held over 20 meetings with a broad range of stakeholders, based on a consultation document. This document was also posted on Justice Canada's website for review and comment by the general public. Over 300 written submissions were received, and a summary of these submissions was released to the public on August 6, 2003.

- In terms of specific stakeholder feedback resulting from the 2002 consultations, the law enforcement community responded by emphasizing the importance of addressing lawful access issues in an expeditious fashion and provided concrete examples of how new technologies and outdated laws are compromising public safety. Industry representatives expressed the view that the consultation document lacked detail and called for further consultation, including the opportunity to comment on the draft legislation prior to introduction in Parliament. Human rights advocates (as well as the federal and some provincial privacy commissioners) were concerned about the scope of the proposals and their potential impact on privacy and civil liberties.

- As a result of this feedback, the proposals were modified and in 2005, additional in-depth consultations (often eight hours in duration) were held with approximately 30 stakeholders, containing a detailed (over 200 pages) presentation based on extracts of the proposed legislation and regulations.

- During these consultations, telecommunication service providers (TSPs) indicated that there is significant common ground between their views and the federal government's proposals, and commented that while they were willing to absorb some costs for public safety, these costs must be kept to a minimum. The industry support for absorbing some capital costs was tied to

an expectation that they would receive compensation for the assistance that they provide in implementing interceptions, and for compliance ordered by the Minister of Public Safety.

- With respect to the industry's reactions to the customer name and address proposals, most industry representatives did not express significant concerns with the proposed administrative nature of the proposals, as it was seen as addressing their primary concern, i.e., when to provide this information. Lack of clarity in this area was the principal concern for most industry stakeholders. Concerns expressed by these stakeholders usually related to the details of proposals such as the timeframe in which they would need to provide customer name and address information and whether they would receive compensation. Only one company consistently expressed concern from a privacy perspective in relation to the proposals (Videotron).

2005 Consultations

- The views of the federal and some provincial Privacy Commissioners (Ontario, Alberta and British Columbia), as well as civil liberties groups, were also obtained during the 2005 consultations. Although specific concerns were allayed by these consultations, such as the fact that the proposals will not prohibit the personal use of encryption, and will not change Canada's 1998 Policy on Cryptography, the Privacy Commissioner of Canada, along with several of her provincial counterparts, and human rights advocates, can be expected to continue to advocate for additional safeguards for privacy, in keeping with their mandates.

- With respect to the customer name and address information proposals, some privacy stakeholders did note with approval that the government was not proposing to require companies to collect and retain information about their subscribers or their communication activities (mandatory data retention); nor to create a national database of such information; nor require these companies to have to verify the identity of their subscribers, as has been done in some other jurisdictions.

- These stakeholders did however express concern about the proposal to provide for law enforcement and CSIS to access customer name and address information without a court authorization. Privacy Commissioners and their officials recommended, at a minimum, that additional administrative and privacy protections be included in the proposed legislation. Privacy advocates such as the B.C. Civil Liberties Association, were clearly of the view that judicial oversight was necessary.

- Following these consultations, the proposals were amended to increase the number of safeguards, as recommended by privacy advocates, which include:

    - limiting the number of designated persons who can request the information to 5 persons or 5% of an agency's employees;
    - designated persons must create a record of all requests;
    - agency heads must ensure regular internal audits and report to their responsible Ministers on those audits.

2006/2007 Consultations

- In 2006/2007, further discussions were undertaken with industry and police representative associations. As a result, amendments were made to the proposed TALEA that will help address privacy concerns including: a review of the legislation by Parliament after five years and clarification of the limited scope of information to be obtained respecting customers.

- [redacted]

TAB D

Proposed List of Stakeholders for 2007 Consultation

Based on a list provided by officials in your office, it is recommended that the following individuals and groups be part of the proposed 2007 consultations on the customer name and address proposals.

Industry:

- Information Technology Association of Canada (Bill Munson)
- The Canadian Wireless Telecommunications Association (CWTA)
- Canadian Association of Internet Providers (CAIP)
- Select representatives from the Canadian Coalition Against Internet Child Exploitation

Consumer/Privacy Advocates/Academics:

- Anver Levin – Ryerson University
- Alicia Wanless – International Perspectives
- Martin Rudner – Carleton University
- Stephen Johnson – Federal Privacy Commission
- Canadian Bar Association
- John Boufford – Canadian Information Processing Society
- Paul-Andre Comeau – Professor (ENAP)
- Michael Geist – Professor (University of Ottawa)

Law Enforcement/Victims and Crime Prevention:

- Royal Canadian Mounted Police (National Child Exploitation Co-ordination Centre)
- Canadian Association of Chiefs of Police
- Toronto Police Service – Project "P"
- Cybertip.ca
- Canadian Resource Centre for Victims of Crime
- B'nai Brith

Public Safety Canada / Sécurité publique Canada

File/Docket No. – N° dossier

ACTION REQUEST / FICHE DE SERVICE

To – À: Lynda Clairmont

Date: Aug 29, 2007

For Signature

Purpose/Urgency – But/Urgence

Lawful Access Consultations

Subject/Remarks – Sujet/Remarques

C.C.:
- ☐ Chantal Bernier
- ☐ J. Scott Broughton/ Lynda Clairmont
- ☐ Richard Wex
- ☐ Kristina Namiesniowski
- ☐ Elisabeth Nadeau
- ☐ Daniel Lavoie
- ☐ Richard Fiutowski

Consultations undertaken / Consultations entreprises :

Legal / Services juridiques _____

Corporate Management / Gestion ministérielle _____

PCO-IGA / BCP-AIG _____

	Name/Signature Nom/Signature	Date
Originator Initiateur	Yacie Touzin	Aug. 29/07
Director Directeur		29-8-07
Deputy Director General Directeur général adjoint		
Director General Directeur général		2007.09.07
SADM/Assoc. ADM, EMNS SMAP/SMA déléguée, GMUSN	J. Scott Broughton/ Lynda Clairmont	Sept 10/07
ADM, CSPB SMA, SPP		
ADM, CMB SMA, GM		
Comptroller Contrôleur		
ADM, PLEIB SMA, SPALI		
ADM, SPB SMA, DPS		
Ministerial Services Division Division des services ministériels		
Associate Deputy Minister Sous-ministre délégué		
Deputy Minister Sous-ministre		

PS-51-E (2/05)

[redacted]

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

6950-1 \ 348139

MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER

CONSULTATION PACKAGE FOR DISTRIBUTION TO SELECT STAKEHOLDERS FOR CONSULTATIONS ON THE ACCESS TO CUSTOMER NAME AND ADDRESS (CNA) INFORMATION COMPONENT OF DRAFT LAWFUL ACCESS LEGISLATION

(For Signature)

SUMMARY

- NSPD officials are moving forward for a series of individual and small group consultations on the issue of access to CNA information by law enforcement and the Canadian Security Intelligence Service (CSIS), targeted to begin September 7th (**TAB A** – draft critical path).

- Attached for your approval and signature are the documents proposed for mail-out to identified stakeholders (**TAB B**) to initiate the consultations:
  - an invitation letter from you to stakeholders (**TAB C**); and,
  - a consultation document that would form the basis for in-person meetings, teleconferences or written input (**TAB D**).

- These documents have been shared with the Privy Council Office, Industry Canada (IC) and Justice Canada [redacted]

- IC has expressed a desire to expand the scope of stakeholders consulted. Once IC's list of stakeholders is confirmed, additional invitation letters will be sent to you for signature.

Scope and Format of Consultations

- Considerable work has taken place in the development of an administrative model for gaining access to CNA information. Current TALEA proposals were informed by broad-based consultations in 2002 and 2005 and more targeted consultations in 2006. They represent a balancing of the needs expressed by law enforcement, industry and privacy groups. The current consultations will focus on this administrative model.

Canada

- Further to direction, small group and individual consultations with select stakeholders are being pursued. Stakeholders will be grouped by sector. Consultations with industry and law enforcement will be split into two separate sessions. Consultations with privacy and civil society advocates will occur in smaller groups as appropriate. Certain high-profile privacy stakeholders will be invited to meet on a one-on-one basis, e.g., the Office of the Privacy Commissioner and the Canadian Bar Association. Consultations will be carried out by teleconference if required.

- As previously advised, it is expected that there may be media attention as a result of the distribution of the consultation document and consultation discussions; some participants may ask for more time to respond, beyond the September 25th deadline indicated in the letters.

- A Question Period note for the Minister is being prepared on the consultations and will be forwarded shortly for approval.

RECOMMENDATIONS

- It is recommended that you approve the consultation document and sign the invitation letters attached (**TAB C** – invitation letters in English and French).

R. Evans
DG, NSPD

Enclosures: (4)

TAB A

DRAFT CRITICAL PATH FOR CONSULTATIONS ON CUSTOMER NAME AND ADDRESS (CNA) INFORMATION

➢ ***Consultation Target Date: September 7 to 25, 2007***

August 31 -	Mail-out consultation packages to stakeholders, comprising Consultation Document and Invitation Letter signed by SADM
September 4 -	Make advance calls to stakeholders regarding interest/availability for consultations
September 4 to 7 -	Create consultation schedule (including date/time/location) based on stakeholder interest/availability; follow up with stakeholders regarding consultation schedule
September 7 to 25 -	Consultations with stakeholders
September 30 -	Draft consultation report provided for DM review

TAB B

Proposed List of Stakeholders for 2007 Consultation

It is recommended that the following individuals and groups be part of the proposed 2007 consultations on the customer name and address proposals.

Industry:

- Information Technology Association of Canada (ITAC)
- The Canadian Wireless Telecommunications Association (CWTA)
- Canadian Association of Internet Providers (CAIP)
- David Elder, Bell Canada
- [Industry Canada to propose additional participants]

Consumer/Privacy Advocates/Academics:

- Avner Levin – Ryerson University
- Alicia Wanless – International Perspectives
- Raymond D'Aoust – Office of the Privacy Commissioner
- Canadian Bar Association
- John Boufford – Canadian Information Processing Society
- Paul-Andre Comeau – Professor (ENAP)
- Michael Geist – Professor (University of Ottawa)

Law Enforcement/Victims and Crime Prevention:

- Royal Canadian Mounted Police (National Child Exploitation Co-ordination Centre)
- Canadian Association of Chiefs of Police (Law Amendments Committee)
- Ontario Provincial Police – Project "P"
- Cybertip.ca
- Canadian Resource Centre for Victims of Crime
- B'nai Brith

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Inspector Andy Stewart
Ontario Provincial Police Child Pornography Section
1201 Wilson Ave., Building E, Suite 224
Downsview, Ontario
M3M 1J8

Dear Inspector Stewart:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should you have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

M. Bernard Amyot
Président, L'association du Barreau canadien
865 Carling Avenue, Suite 500
Ottawa, Ontario K1S 5S8

Monsieur Amyot,

Sécurité publique Canada aimerait obtenir, au cours des semaines à venir, vos commentaires sur les mesures à prendre pour répondre aux exigences en matière d'accès légal des organismes responsables de l'application de la loi et de la sécurité nationale, relativement aux renseignements sur les noms et adresses des clients que tiennent les fournisseurs des services de télécommunications.

Pour votre examen, vous trouverez ci-joint le document de travail qui servira de base aux discussions. L'accès légal a fait l'objet de deux séances de consultation avec les intervenants en 2002 et 2005. Comme indiqué dans le document ci-joint, les prochaines consultations porteront exclusivement sur les approches qui permettraient aux organismes responsables de l'application de la loi et de la sécurité nationale d'obtenir l'accès nécessaire aux noms et adresses des clients, tout en assurant la protection des renseignements personnels.

Vos commentaires sur toute question relative au document de travail seront les bienvenus. Des téléconférences ou des réunions en personne se tiendront prochainement à Ottawa. Vous pouvez également soumettre vos commentaires par écrit à l'adresse mentionnée dans le document ci-joint. Dans cette éventualité, veuillez transmettre vos commentaires écrits avant le 25 septembre 2007.

Si vous ou votre organisation désirez participer aux consultations, je vous invite à communiquer avec Mme Amanda Tait, agente chargée des politiques, au numéro de téléphone ou à l'adresse électronique suivants : 613 949-3184, Amanda.tait@ps.gc.ca.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Vous êtes également invité à communiquer avec Mme Tait pour obtenir des renseignements supplémentaires et confirmer votre participation.

Je vous remercie de l'intérêt que vous portez à cette importante question de sécurité publique, et c'est avec plaisir que j'attends vos commentaires.

Veillez agréer mes salutations les plus distinguées.

Lynda Clairmont
Sous-ministre adjoint associée
Secteur de la gestion des mesures
d'urgence et sécurité nationale

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

M. Raymond D'Aoust
Commissaire adjoint à la protection de la vie privée
Commissariat à la protection de la vie privée du Canada
112 Kent Street, Suite 300
Ottawa, Ontario K1A 1H3

Monsieur D'Aoust,

Sécurité publique Canada aimerait obtenir, au cours des semaines à venir, vos commentaires sur les mesures à prendre pour répondre aux exigences en matière d'accès légal des organismes responsables de l'application de la loi et de la sécurité nationale, relativement aux renseignements sur les noms et adresses des clients que tiennent les fournisseurs des services de télécommunications.

Pour votre examen, vous trouverez ci-joint le document de travail qui servira de base aux discussions. L'accès légal a fait l'objet de deux séances de consultation avec les intervenants en 2002 et 2005. Comme indiqué dans le document ci-joint, les prochaines consultations porteront exclusivement sur les approches qui permettraient aux organismes responsables de l'application de la loi et de la sécurité nationale d'obtenir l'accès nécessaire aux noms et adresses des clients, tout en assurant la protection des renseignements personnels.

Vos commentaires sur toute question relative au document de travail seront les bienvenus. Des téléconférences ou des réunions en personne se tiendront prochainement à Ottawa. Vous pouvez également soumettre vos commentaires par écrit à l'adresse mentionnée dans le document ci-joint. Dans cette éventualité, veuillez transmettre vos commentaires écrits avant le 25 septembre 2007.

Si vous ou votre organisation désirez participer aux consultations, je vous invite à communiquer avec Mme Amanda Tait, agente chargée des politiques, au numéro de téléphone ou à l'adresse électronique suivants : 613 949-3184, Amanda.tait@ps.gc.ca.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Vous êtes également invité à communiquer avec Mme Tait pour obtenir des renseignements supplémentaires et confirmer votre participation.

Je vous remercie de l'intérêt que vous portez à cette importante question de sécurité publique, et c'est avec plaisir que j'attends vos commentaires.

Veillez agréer mes salutations les plus distinguées.

L Clairmont

Lynda Clairmont
Sous-ministre adjoint associée
Secteur de la gestion des mesures
d'urgence et sécurité nationale

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

M. Paul-André Comeau
Professeur invite, École nationale d'administration publique
373 Sussex Drive
Ottawa, Ontario, Canada
K1N 6Z2

Monsieur Comeau,

Sécurité publique Canada aimerait obtenir, au cours des semaines à venir, vos commentaires sur les mesures à prendre pour répondre aux exigences en matière d'accès légal des organismes responsables de l'application de la loi et de la sécurité nationale, relativement aux renseignements sur les noms et adresses des clients que tiennent les fournisseurs des services de télécommunications.

Pour votre examen, vous trouverez ci-joint le document de travail qui servira de base aux discussions. L'accès légal a fait l'objet de deux séances de consultation avec les intervenants en 2002 et 2005. Comme indiqué dans le document ci-joint, les prochaines consultations porteront exclusivement sur les approches qui permettraient aux organismes responsables de l'application de la loi et de la sécurité nationale d'obtenir l'accès nécessaire aux noms et adresses des clients, tout en assurant la protection des renseignements personnels.

Vos commentaires sur toute question relative au document de travail seront les bienvenus. Des téléconférences ou des réunions en personne se tiendront prochainement à Ottawa. Vous pouvez également soumettre vos commentaires par écrit à l'adresse mentionnée dans le document ci-joint. Dans cette éventualité, veuillez transmettre vos commentaires écrits avant le 25 septembre 2007.

Si vous désirez participer aux consultations, je vous invite à communiquer avec Mme Amanda Tait, agente chargée des politiques, au numéro de téléphone ou à l'adresse électronique suivants : 613 949-3184, Amanda.tait@ps.gc.ca.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Vous êtes également invité à communiquer avec Mme Tait pour obtenir des renseignements supplémentaires et confirmer votre participation.

Je vous remercie de l'intérêt que vous portez à cette importante question de sécurité publique, et c'est avec plaisir que j'attends vos commentaires.

Veillez agréer mes salutations les plus distinguées.

Lynda Clairmont
Sous-ministre adjoint associée
Secteur de la gestion des mesures d'urgence et sécurité nationale

Canada

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Deputy Commissioner Peter Martin
Royal Canadian Mounted Police
RCMP Headquarters, Nicholson Building
1200 Vanier Parkway, Room G322
K1A 0R2

Dear Deputy Commissioner Peter Martin:

Public Safety Canada will be seeking the input of the National Child Exploitation Coordination Centre over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments bySeptember 25, 2007.

Should the NCECC have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

L Clairmont

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Canada

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Professor Michael Geist
Canada Research Chair in Internet and E-commerce Law
University of Ottawa, Faculty of Law, Common Law Section
57 Louis Pasteur, Box 450, Stn. A
Ottawa, ON K1N 6N5

Dear Professor Geist:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should you have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Canada

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Deputy Chief Constable Clayton Pecknold and
Assistant Director Pierre-Paul Pichette
Co-Chairs, Law Amendments Committee
Canadian Association of Chiefs of Police
582 Somerset St. W
Ottawa, ON
K1R 5K2

Dear Deputy Chief Constable Pecknold and Assistant Director Pichette:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Should the Canadian Association of Chiefs of Police have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

L Clairmont

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Canada

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Mr. Avner Levin
Faculty of Business
Ryerson University
350 Victoria Street
Toronto, Ontario
M5B 2K3

Dear Mr. Levin:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Should you have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Canada

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Mr. Michael Mostyn
Director of Government Relations, B'nai Brith Canada
Fuller Bldg. 75 Albert Street
Ottawa, Ontario K1P 5E7

Dear Mr. Mostyn:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should B'nai Brith Canada have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Canada

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Signy Arnason
Director, Canadian Centre for Child Protection
615 Academy Road
Winnipeg, Manitoba
R3N 0E7

Dear Ms. Arnason:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should Cybertip have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Mr. Peter Barnes
President and CEO
Canadian Wireless Telecommunications Association
1110-130 Albert Street
Ottawa, Ontario K1P 5G4

Dear Mr. Barnes:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Should the Canadian Wireless Telecommunications Association have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Alicia Wanless
Executive Director, International Perspectives
10 Shallmar Blvd., Suite 1008
Toronto, ON
M5N 1J4

Dear Ms. Wanless:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should you have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

L Clairmont

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Mr. Tom Copeland
Chair
Canadian Association of Internet Providers
388 Albert Street, 2nd Floor
Ottawa, Ontario K1R 5B2

Dear Mr. Copeland:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should the Canadian Association of Internet Providers have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Canada

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Mr. John Boufford
President, Canadian Information Processing Society
5090 Explorer Drive, Suite 801
Mississauga, Ontario L4W 4T9

Dear Mr. Boufford:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should the Canadian Information Processing Society have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Canada

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Mr. Bernard Courtois
President and CEO
Information Technology Association of Canada
220 Laurier Ave. W, Suite 1120
Ottawa, ON K1P 5Z9

Dear Mr. Courtois:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Should the Information Technology Association of Canada have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

L Clairmont

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Canada

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Mr. David B. Elder
Vice President, Regulatory Law
Bell Canada
110 O'Connor Street, 7th floor
Ottawa, Ontario K1P 1H1

Dear Mr. Elder:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should Bell Canada have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Canada

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Heidi Illingworth
Executive Director, Canadian Resource Centre for Victims of Crime
100 - 141 Catherine Street
Ottawa, ON
K2P 1C3

Dear Ms. Illingworth:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Canada

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Should the Canadian Resource Centre for Victims of Crime have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Canada

CUSTOMER NAME AND ADDRESS (CNA) INFORMATION CONSULTATION DOCUMENT

INTRODUCTION

Modern telecommunications and computer networks such as the Internet are a great source of economic and social benefits, but they can also be used in the planning, coordination, financing and perpetration of crimes and threats to public safety and the national security of Canada. By extension, the rapidly evolving nature of these technologies can pose a significant challenge to law enforcement and national security officials who are entrusted with combating these threats, and who employ lawful access to communications and information to do so.

The principles and powers of lawful access must be exercised in a manner consistent with the rights and freedoms guaranteed in the *Canadian Charter of Rights and Freedoms* and while adapting to the rapid pace of technological change.

THE CONSULTATION PROCESS

Public Safety Canada, in collaboration with Industry Canada, is presently examining how to address the challenges faced by police, the Canadian Security Intelligence Service (CSIS) and the Competition Bureau when seeking timely access to basic CNA information in a modern telecommunications milieu. This question was previously considered by stakeholders in broader consultation processes on lawful access issues held in 2002 and 2005.

The purpose of this consultation is to provide a range of stakeholders - including police and industry representatives and groups interested in privacy and victims of crime issues - with an opportunity to identify their current views on possible approaches to updating Canada's lawful access provisions as they relate to law enforcement and national security officials' need to gain access to CNA information in the course of their duties. 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.

The objectives of this process are to maintain lawful access for law enforcement and national security agencies in the face of new technologies while preserving and protecting the privacy and other rights and freedoms of all people in Canada. In striving to attain these goals, it is essential to ensure that the competitiveness of Canadian industry is taken into account and that the solutions adopted do not place an unreasonable burden on the Canadian public.

CURRENT CONTEXT

Timely access to CNA information is an important tool used by law enforcement and national security agencies to fulfil their public safety mandates. This type of information can be vital in the context of investigations of online criminal activity, such as child exploitation.

Law enforcement agencies have been experiencing difficulties in consistently obtaining basic CNA information from telecommunications service providers (TSPs). In the absence of explicit legislation, a variety of practices exists among TSPs with respect to the release of basic customer information, e.g., name, address, telephone number, or their Internet equivalents. Some companies provide this information voluntarily, while others require a warrant before providing any information, regardless of its nature or the nature of the situation. 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. This poses a problem in some contexts. For example, law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation. The availability of such building-block information is often the difference between the start and finish of an investigation.

CNA INFORMATION

In the context of options under consideration by Public Safety Canada and its partner departments and agencies, CNA information refers to basic identifiers that would assist law enforcement and national security agencies to determine the identity of a telecommunications service subscriber, if this information was necessary to the performance of their duties.

The scope of CNA information obtained could include the following basic identifiers associated with a particular subscriber:

- name;
- address(es);
- ten-digit telephone numbers (wireline and wireless);
- Cell phone identifiers, e.g., one or more of several unique identifiers associated with a subscriber to a particular telecommunications service (mobile identification number or MIN; electronic serial number or ESN; international mobile equipment or IMEI number; international mobile subscriber identity or IMSI number; subscriber identity module card number of SIM Card Number);
- e-mail address(es);

- IP address; and/or,

- Local Service Provider Identifier, i.e., identification of the TSP that owns the telephone number or IP address used by a specific customer.

POSSIBLE MODEL

Options based on an administrative model are being considered closely by officials.

POSSIBLE SAFEGUARDS

Further to input received during 2002 and 2005 consultations, a number of safeguards could be included under a possible administrative model requiring the release of limited basic CNA information to law enforcement and national security agencies upon request. These could include:

- clear limitations on what customer information could be obtained upon request;

- limiting the number of employees who would have access to CNA;

- requiring that individuals with access be designated by senior officials within their organizations;

- limiting requests to those made for the purpose of performing an official duty or function;

- requiring that requests be made in writing, except in exceptional circumstances;

- requiring that designated officials provide associated information with their request, e.g., identification of a specific date and time for a request relating to an IP address;

- requiring designated officials to record their status as such when making a request, as well as the duty or function for which a particular request is made;

- limiting the use of any information obtained to the agency that obtained it for the purpose for which the information was obtained, or for a use consistent with that purpose, unless permission is granted by the individual to whom it relates;

- requiring regular internal audits by agency heads to ensure that any requests for CNA information are being made in accordance with the protocols and safeguards in place;

- reporting to responsible ministers on the result of any internal audits;

- provision of any audit results to the Privacy Commissioner of Canada, the Security Intelligence Review Committee, or provincial privacy commissioners, as appropriate;

- provision for the Privacy Commissioner and SIRC to conduct audits related to the release of CNA information.

Under no option being examined would TSPs be compelled to track the actions of customers or to collect information about them in the absence of necessary court authorizations governing such activity in Canada, nor would law enforcement or national security agencies be permitted to obtain the content of a customer's communications without such authorizations.

CONCLUSION

Officials plan to meet with a range of interested parties in September, 2007 to discuss the issues raised in this paper.

Written comments may also be sent to the following address by September 25, 2007, and will be gratefully received:

Customer Name and Address Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON, Canada K1A 0P8

INFORMATION SUR LES NOMS ET ADRESSES DES CLIENTS DOCUMENT DE CONSULTATION

INTRODUCTION

Les nouveaux systèmes de télécommunications et réseaux informatiques comme Internet génèrent d'importants avantages économiques et sociaux. Par contre, ils peuvent également servir à planifier, à coordonner, à financer et à commettre des crimes ainsi qu'à menacer la sécurité publique et nationale du Canada. En raison de leur évolution rapide, ces technologies peuvent causer d'importants problèmes aux responsables de l'application de la loi et de la sécurité nationale qui doivent lutter contre ces menaces et qui, pour se faire, doivent appliquer les principes de l'accès légal aux communications et à l'information.

Les principes et les pouvoirs relatifs à l'accès légal doivent être exercés de façon à respecter les droits et les libertés garantis par la Chartre canadienne des droits et libertés, tout en étant adaptés au rythme rapide de l'évolution des technologies.

LE PROCESSUS DE CONSULTATION

Sécurité publique Canada, en collaboration avec Industrie Canada, examine présentement comment les services de police, le Service canadien du renseignement de sécurité (SCRS) et le Bureau de la concurrence peuvent surmonter les difficultés auxquelles ils doivent faire face lorsqu'ils doivent obtenir de l'information de base sur les noms et adresses des clients, dans le contexte des technologies modernes des télécommunications. Cette question a déjà fait l'objet d'un examen des intervenants, dans le cadre de processus de consultations plus vastes sur l'accès légal, tenues en 2002 et en 2005.

Ces consultations ont pour but de permettre à une vaste gamme de parties intéressées, comme les services de police, l'industrie ainsi que les organismes de défense des libertés civiles et des victimes de crime, de donner leur point de vue sur les démarches possibles qui visent la mise à jour des dispositions canadiennes en matière d'accès légal, en ce qui concerne la nécessité des responsables de l'application de la loi et de la sécurité nationale d'obtenir de l'information sur les noms et adresses des clients dans le cadre de leurs tâches quotidiennes. L'étendue possible de l'information sur les noms et adresses des clients à obtenir est expliquée dans ce document de consultation, mais il faut préciser dès le départ que cette information ne comprendrait d'aucune façon le contenu des communications des clients ou les sites Internet qu'ils ont consultés.

Les objectifs de ce processus visent à maintenir l'accès légal pour les organismes responsables de l'application de la loi et de la sécurité nationale dans le contexte du développement constant de nouvelles technologies, tout en préservant et en assurant la protection de la vie privée ainsi que les autres droits et libertés de toutes les personnes habitant au Canada. La réalisation de ces objectifs doit absolument prendre en compte le fait que l'industrie canadienne doit demeurer concurrentielle et que les solutions adoptées ne doivent pas représenter un fardeau déraisonnable pour le public canadien.

CONTEXTE ACTUEL

L'accès rapide à l'information sur les noms et adresses des clients est un outil important dont se servent les organismes chargés de l'application de la loi et de la sécurité nationale pour s'acquitter de leur mandat touchant la sécurité publique. Lorsqu'il est question d'enquêtes portant sur des cybercrimes, tel que l'exploitation des enfants, ce type d'information peut s'avérer vital.

Il est difficile pour les organismes d'application de la loi d'obtenir des fournisseurs de services de télécommunication, de façon constante, l'information de base sur les noms et adresses des clients. Sans dispositions législatives explicites, les différents fournisseurs de services de télécommunication observent toute une gamme de pratiques en ce qui a trait à la divulgation de l'information de base sur le client, notamment le nom, l'adresse, le numéro de téléphone ou leurs équivalents sur Internet. Certaines entreprises divulguent volontairement cette information, alors que d'autres exigent qu'un mandat soit présenté avant de fournir l'information demandée, quelle que soit la nature de cette information ou le contexte entourant la demande. Si le gardien de l'information refuse de coopérer lorsqu'une demande est faite pour obtenir cette information, les organismes chargés de faire appliquer la loi n'ont aucun moyen d'exiger la production des renseignements relatifs au client, ce qui peut poser problème dans certains cas. Par exemple, les organismes d'application de la loi peuvent avoir besoin de l'information pour des raisons non reliées à une enquête (c.-à-d. pour trouver le plus proche parent en cas d'urgence) ou parce qu'il s'agit d'un début d'enquête. Le fait d'avoir accès à cette information de base constitue souvent la différence entre le début d'une enquête ou sa fin.

INFORMATION SUR LES NOMS ET ADRESSES DES CLIENTS

Dans le contexte des options examinées par les représentants de Sécurité publique Canada et des ministères et organismes partenaires, l'information sur les noms et adresses des clients renvoie aux identificateurs de base qui pourraient aider les organismes responsables de l'application de la loi et de la sécurité nationale à déterminer l'identité d'un abonné d'un service de télécommunication, si cette information était nécessaire à l'exécution de leurs fonctions.

L'information obtenue sur les noms et adresses d'un abonné d'un service de télécommunication en particulier pourrait comprendre les identificateurs de base suivants:

- nom;
- adresse(s);
- numéro de téléphone de dix chiffres (service conventionnel à fil ou service sans fil);

- identificateurs de téléphone cellulaire, c.-à-d. un ou plusieurs identificateurs uniques associés à un abonné d'un service particulier de télécommunication (numéro d'identification de service mobile; numéro de série électronique; identité internationale d'équipement mobile; identité internationale d'abonné mobile; numéro de carte de module d'identité d'abonné ou numéro de carte SIM);

- adresse(s) de courriel;

- adresses IP;

- identificateur du fournisseur de services locaux, c.-à-d. identification du fournisseur de services de télécommunication à qui appartient le numéro de téléphone ou l'adresse IP dont se sert un client en particulier.

MODÈLE POSSIBLE

Les responsables du dossier examinent soigneusement des options fondées sur un modèle administratif.

MESURES POSSIBLES DE SÉCURITÉ

Conformément aux commentaires reçus à l'issue des consultations tenues en 2002 et en 2005, un certain nombre de mesures de sécurité seraient incluses dans le modèle administratif envisagé, selon lequel les fournisseurs de services de télécommunication seraient tenus de divulguer, à la demande des organismes responsables de l'application de la loi et de la sécurité nationale, des renseignements de base limités sur les noms et adresses des clients. Comme mesures de sécurité, on pourrait :

- établir des restrictions claires concernant le type d'information sur le client qu'il est possible d'obtenir sur demande;

- fixer une limite du nombre d'employés ayant accès à l'information sur les noms et adresses des clients;

- exiger que les personnes ayant accès à l'information soient nommées par les cadres supérieurs de leur organisme;

- exiger que les demandes soient limitées à celles ayant trait à l'exécution d'une tâche ou d'une fonction officielle;

- exiger que ces demandes soient présentées par écrit, à moins de circonstances exceptionnelles;

- exiger que les agents désignés fournissent de l'information connexe avec leur demande, comme la date ou l'heure précise pour une demande concernant une adresse IP;

- exiger des agents désignés qu'ils s'identifient comme agent désigné sur la demande, et qu'ils donnent la tâche ou la fonction à l'origine de la demande;

- empêcher l'organisme demandeur d'utiliser toute information obtenue à une fin connexe ou autre que celle invoquée en vue de son obtention, à moins que la personne visée n'ait accordé son autorisation pour une utilisation supplémentaire;

- exiger que les chefs de l'organisme effectuent régulièrement des vérifications internes afin de veiller à ce que les demandes d'information sur les noms et adresses des clients soient bien conformes aux protocoles et aux mesures de sécurité mis en place;

- transmettre les résultats des vérifications internes aux ministres responsables;

- transmettre les résultats des vérifications au Commissaire à la protection de la vie privée du Canada, au Comité de surveillance des activités de renseignement de sécurité (CSARS) et aux commissaires provinciaux à la protection de la vie privée, s'il y a lieu;

- permettre au Commissaire à la protection de la vie privée du Canada et au CSARS d'effectuer des vérifications ayant trait à la divulgation de l'information sur les noms et adresses des clients;

Aucune des options actuellement en examen n'exige des fournisseurs de services de télécommunication qu'ils effectuent un suivi des actions de leurs clients ou recueillent des données sur ceux-ci sans avoir obtenu les autorisations requises du tribunal gouvernant de telles activités au Canada. De plus, les organismes responsables de l'application de la loi ou de la sécurité nationale ne pourraient pas accéder au contenu des communications d'un client sans avoir l'autorité pertinente.

CONCLUSION

Les responsables planifient de rencontrer les diverses parties intéressées en septembre 2007, afin de discuter les éléments énoncés dans ce document.
Nous vous saurions gré de nous transmettre vos commentaires écrits d'ici le 25 septembre 2007, à l'adresse suivante :

Consultations sur les noms et adresses des clients
Sécurité publique Canada
269, avenue Laurier Ouest, bureau 16C
Ottawa (Ontario) K1A 0P8
Canada

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Pls ensure min's office is fully briefed. Pls also brief Comms.

PROTECTED

DATE: SEP 10 2007

6950-1/18291/347745

MEMORANDUM FOR THE DEPUTY MINISTER

Fuy 10/9/07

UPDATE ON CONSULTATIONS REGARDING THE ACCESS TO CUSTOMER NAME AND ADDRESS INFORMATION COMPONENT [redacted]

Not relevant

(For Information)

SUMMARY

- The Emergency Management and National Security Branch is proceeding with consultations on the issue of access to customer name and address (CNA) information by law enforcement and the Canadian Security Intelligence Service (CSIS).

- Attached for your information are the documents mailed out to identified stakeholders in advance of consultations: an invitation letter from the Senior Assistant Deputy Minister's Office to stakeholders (**TAB A**); a document that forms the basis for subsequent in-person meetings, teleconferences, or written input (**TAB B**); and the proposed list of stakeholders (**TAB C**).

- Draft documents have been shared with Privy Council Office (PCO), Industry Canada (IC), and Department of Justice (DOJ). Comments received have been integrated.

BACKGROUND

- Considerable work has taken place in the development of an administrative model for gaining access to CNA information. Current TALEA proposals were informed by broad-based consultations in 2002 and 2005, and more targeted consultations in 2006, and represent a balancing of the needs expressed by law enforcement, industry and privacy groups. The present consultations focus on the TALEA model,

which is administrative in nature (as opposed to a judicial, warrant-based model), and seek to confirm stakeholders' views and/or obtain any new views or insights on the issue.

- Both small group and individual consultations with select stakeholders are being pursued (a list of participants established based on input from the Minister's Office, PCO and IC).

- Delays forced a change in the consultation timeline, particularly waiting for comments from IC and PCO. Following the Cabinet shuffle, IC asked that the consultation process be delayed to allow for more time to brief Minister Prentice on the consultations. Discussions ultimately took place between this office and IC regarding the consultation strategy and IC agreed to proceed on August 29th.

CONSIDERATIONS

- Law enforcement stakeholders will continue to raise concerns that the government is not proceeding quickly enough with legislation. Privacy advocates will likely criticize the government for not pursuing a warrant-based regime for access to CNA information. Industry stakeholders will cautiously acknowledge law enforcement's needs in this area; however, some may also cite their customers' privacy rights as a concern.

- The consultation process may result in media coverage (e.g. the consultation document might be subject to coverage). Negative reactions can be expected from privacy stakeholders who oppose the CNA proposals.

- Officials from IC, DOJ, RCMP and CSIS will participate in the consultations, to support full and effective discussion of the issues at hand.

COMMENT

- The consultations are targeted to conclude before the end of September.

Lynda Clairmont
Associate ADM

J. Scott Broughton
Senior ADM

Emergency Management and National Security

Enclosures: (3)

TAB A

Sample Invitation Letter to Stakeholders (Generic)

Dear [Recipient's Name Here]:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should **you/your organization (tailor)** have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

(Madame) (Monsieur),

Sécurité publique Canada aimerait obtenir, au cours des semaines à venir, vos commentaires sur les mesures à prendre pour répondre aux exigences en matière d'accès légal des organismes responsables de l'application de la loi et de la sécurité nationale, relativement aux renseignements sur les noms et adresses des clients que tiennent les fournisseurs des services de télécommunications.

Pour votre examen, vous trouverez ci-joint le document de travail qui servira de base aux discussions. L'accès légal a fait l'objet de deux séances de consultation avec les intervenants en 2002 et 2005. Comme indiqué dans le document ci-joint, les prochaines consultations porteront exclusivement sur les approches qui permettraient aux organismes responsables de l'application de la loi et de la sécurité nationale d'obtenir l'accès nécessaire aux noms et adresses des clients, tout en assurant la protection des renseignements personnels.

Vos commentaires sur toute question relative au document de travail seront les bienvenus. Des téléconférences ou des réunions en personne se tiendront prochainement à Ottawa. Vous pouvez également soumettre vos commentaires par écrit à l'adresse mentionnée dans the document ci-joint. Dans cette éventualité, veuillez transmettre vos commentaires écrits avant le 25 septembre 2007.

Si vous ou votre organisation désirez participer aux consultations, je vous invite à communiquer avec Mme Amanda Tait, agente chargée des politiques, au numéro de téléphone ou à l'adresse électronique suivants : 613 949-3184, Amanda.tait@ps.gc.ca. Vous êtes également invitée à communiquer avec Mme Tait pour obtenir des renseignements supplémentaires et confirmer votre participation.

Je vous remercie de l'intérêt que vous portez à cette importante question de sécurité publique, et c'est avec plaisir que j'attends vos commentaires.

Veillez agréer mes salutations les plus distinguées.

Lynda Clairmont
Sous-ministre adjoint associée
Secteur de la gestion des mesures
d'urgence et sécurité national

TAB B

CUSTOMER NAME AND ADDRESS (CNA) INFORMATION CONSULTATION DOCUMENT

INTRODUCTION

Modern telecommunications and computer networks such as the Internet are a great source of economic and social benefits, but they can also be used in the planning, coordination, financing and perpetration of crimes and threats to public safety and the national security of Canada. By extension, the rapidly evolving nature of these technologies can pose a significant challenge to law enforcement and national security officials who are entrusted with combating these threats, and who employ lawful access to communications and information to do so.

The principles and powers of lawful access must be exercised in a manner consistent with the rights and freedoms guaranteed in the *Canadian Charter of Rights and Freedoms* and while adapting to the rapid pace of technological change.

THE CONSULTATION PROCESS

Public Safety Canada, in collaboration with Industry Canada, is presently examining how to address the challenges faced by police, the Canadian Security Intelligence Service (CSIS) and the Competition Bureau when seeking timely access to basic CNA information in a modern telecommunications milieu. This question was previously considered by stakeholders in broader consultation processes on lawful access issues held in 2002 and 2005.

The purpose of this consultation is to provide a range of stakeholders - including police and industry representatives and groups interested in privacy and victims of crime issues - with an opportunity to identify their current views on possible approaches to updating Canada's lawful access provisions as they relate to law enforcement and national security officials' need to gain access to CNA information in the course of their duties. 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.

The objectives of this process are to maintain lawful access for law enforcement and national security agencies in the face of new technologies while preserving and protecting the privacy and other rights and freedoms of all people in Canada. In striving to attain these goals, it is essential to ensure that the competitiveness of Canadian industry is taken into account and that the solutions adopted do not place an unreasonable burden on the Canadian public.

CURRENT CONTEXT

Timely access to CNA information is an important tool used by law enforcement and national security agencies to fulfil their public safety mandates. This type of information can be vital in the context of investigations of online criminal activity, such as child exploitation.

Law enforcement agencies have been experiencing difficulties in consistently obtaining basic CNA information from telecommunications service providers (TSPs). In the absence of explicit legislation, a variety of practices exists among TSPs with respect to the release of basic customer information, e.g., name, address, telephone number, or their Internet equivalents. Some companies provide this information voluntarily, while others require a warrant before providing any information, regardless of its nature or the nature of the situation. 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. This poses a problem in some contexts. For example, law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation. The availability of such building-block information is often the difference between the start and finish of an investigation.

CNA INFORMATION

In the context of options under consideration by Public Safety Canada and its partner departments and agencies, CNA information refers to basic identifiers that would assist law enforcement and national security agencies to determine the identity of a telecommunications service subscriber, if this information was necessary to the performance of their duties.

The scope of CNA information obtained could include the following basic identifiers associated with a particular subscriber:

- name;
- address(es);
- ten-digit telephone numbers (wireline and wireless);
- Cell phone identifiers, e.g., one or more of several unique identifiers associated with a subscriber to a particular telecommunications service (mobile identification number or MIN; electronic serial number or ESN; international mobile equipment or IMEI number; international mobile subscriber identity or IMSI number; subscriber identity module card number of SIM Card Number);
- e-mail address(es);

- IP address; and/or,

- Local Service Provider Identifier, i.e., identification of the TSP that owns the telephone number or IP address used by a specific customer.

POSSIBLE MODEL

Options based on an administrative model are being considered closely by officials.

POSSIBLE SAFEGUARDS

Further to input received during 2002 and 2005 consultations, a number of safeguards could be included under a possible administrative model requiring the release of limited basic CNA information to law enforcement and national security agencies upon request. These could include:

- clear limitations on what customer information could be obtained upon request;

- limiting the number of employees who would have access to CNA;

- requiring that individuals with access be designated by senior officials within their organizations;

- limiting requests to those made for the purpose of performing an official duty or function;

- requiring that requests be made in writing, except in exceptional circumstances;

- requiring that designated officials provide associated information with their request, e.g., identification of a specific date and time for a request relating to an IP address;

- requiring designated officials to record their status as such when making a request, as well as the duty or function for which a particular request is made;

- limiting the use of any information obtained to the agency that obtained it for the purpose for which the information was obtained, or for a use consistent with that purpose, unless permission is granted by the individual to whom it relates;

- requiring regular internal audits by agency heads to ensure that any requests for CNA information are being made in accordance with the protocols and safeguards in place;

- reporting to responsible ministers on the result of any internal audits;

- provision of any audit results to the Privacy Commissioner of Canada, the Security Intelligence Review Committee, or provincial privacy commissioners, as appropriate;

- provision for the Privacy Commissioner and SIRC to conduct audits related to the release of CNA information.

Under no option being examined would TSPs be compelled to track the actions of customers or to collect information about them in the absence of necessary court authorizations governing such activity in Canada, nor would law enforcement or national security agencies be permitted to obtain the content of a customer's communications without such authorizations.

CONCLUSION

Officials plan to meet with a range of interested parties in September, 2007 to discuss the issues raised in this paper.

Written comments may also be sent to the following address by September 25, 2007, and will be gratefully received:

Customer Name and Address Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON, Canada K1A 0P8

INFORMATION SUR LES NOMS ET ADRESSES DES CLIENTS DOCUMENT DE CONSULTATION

INTRODUCTION

Les nouveaux systèmes de télécommunications et réseaux informatiques comme Internet génèrent d'importants avantages économiques et sociaux. Par contre, ils peuvent également servir à planifier, à coordonner, à financer et à commettre des crimes ainsi qu'à menacer la sécurité publique et nationale du Canada. En raison de leur évolution rapide, ces technologies peuvent causer d'importants problèmes aux responsables de l'application de la loi et de la sécurité nationale qui doivent lutter contre ces menaces et qui, pour se faire, doivent appliquer les principes de l'accès légal aux communications et à l'information.

Les principes et les pouvoirs relatifs à l'accès légal doivent être exercés de façon à respecter les droits et les libertés garantis par la Chartre canadienne des droits et libertés, tout en étant adaptés au rythme rapide de l'évolution des technologies.

LE PROCESSUS DE CONSULTATION

Sécurité publique Canada, en collaboration avec Industrie Canada, examine présentement comment les services de police, le Service canadien du renseignement de sécurité (SCRS) et le Bureau de la concurrence peuvent surmonter les difficultés auxquelles ils doivent faire face lorsqu'ils doivent obtenir de l'information de base sur les noms et adresses des clients, dans le contexte des technologies modernes des télécommunications. Cette question a déjà fait l'objet d'un examen des intervenants, dans le cadre de processus de consultations plus vastes sur l'accès légal, tenues en 2002 et en 2005.

Ces consultations ont pour but de permettre à une vaste gamme de parties intéressées, comme les services de police, l'industrie ainsi que les organismes de défense des libertés civiles et des victimes de crime, de donner leur point de vue sur les démarches possibles qui visent la mise à jour des dispositions canadiennes en matière d'accès légal, en ce qui concerne la nécessité des responsables de l'application de la loi et de la sécurité nationale d'obtenir de l'information sur les noms et adresses des clients dans le cadre de leurs tâches quotidiennes. L'étendue possible de l'information sur les noms et adresses des clients à obtenir est expliquée dans ce document de consultation, mais il faut préciser dès le départ que cette information ne comprendrait d'aucune façon le contenu des communications des clients ou les sites Internet qu'ils ont consultés.

Les objectifs de ce processus visent à maintenir l'accès légal pour les organismes responsables de l'application de la loi et de la sécurité nationale dans le contexte du développement constant de nouvelles technologies, tout en préservant et en assurant la protection de la vie privée ainsi que les autres droits et libertés de toutes les personnes habitant au Canada. La réalisation de ces objectifs doit absolument prendre en compte le fait que l'industrie canadienne doit demeurer concurrentielle et que les solutions adoptées ne doivent pas représenter un fardeau déraisonnable pour le public canadien.

CONTEXTE ACTUEL

L'accès rapide à l'information sur les noms et adresses des clients est un outil important dont se servent les organismes chargés de l'application de la loi et de la sécurité nationale pour s'acquitter de leur mandat touchant la sécurité publique. Lorsqu'il est question d'enquêtes portant sur des cybercrimes, tel que l'exploitation des enfants, ce type d'information peut s'avérer vital.

Il est difficile pour les organismes d'application de la loi d'obtenir des fournisseurs de services de télécommunication, de façon constante, l'information de base sur les noms et adresses des clients. Sans dispositions législatives explicites, les différents fournisseurs de services de télécommunication observent toute une gamme de pratiques en ce qui a trait à la divulgation de l'information de base sur le client, notamment le nom, l'adresse, le numéro de téléphone ou leurs équivalents sur Internet. Certaines entreprises divulguent volontairement cette information, alors que d'autres exigent qu'un mandat soit présenté avant de fournir l'information demandée, quelle que soit la nature de cette information ou le contexte entourant la demande. Si le gardien de l'information refuse de coopérer lorsqu'une demande est faite pour obtenir cette information, les organismes chargés de faire appliquer la loi n'ont aucun moyen d'exiger la production des renseignements relatifs au client, ce qui peut poser problème dans certains cas. Par exemple, les organismes d'application de la loi peuvent avoir besoin de l'information pour des raisons non reliées à une enquête (c.-à-d. pour trouver le plus proche parent en cas d'urgence) ou parce qu'il s'agit d'un début d'enquête. Le fait d'avoir accès à cette information de base constitue souvent la différence entre le début d'une enquête ou sa fin.

INFORMATION SUR LES NOMS ET ADRESSES DES CLIENTS

Dans le contexte des options examinées par les représentants de Sécurité publique Canada et des ministères et organismes partenaires, l'information sur les noms et adresses des clients renvoie aux identificateurs de base qui pourraient aider les organismes responsables de l'application de la loi et de la sécurité nationale à déterminer l'identité d'un abonné d'un service de télécommunication, si cette information était nécessaire à l'exécution de leurs fonctions.

L'information obtenue sur les noms et adresses d'un abonné d'un service de télécommunication en particulier pourrait comprendre les identificateurs de base suivants:

- nom;
- adresse(s);
- numéro de téléphone de dix chiffres (service conventionnel à fil ou service sans fil);

- identificateurs de téléphone cellulaire, c.-à-d. un ou plusieurs identificateurs uniques associés à un abonné d'un service particulier de télécommunication (numéro d'identification de service mobile; numéro de série électronique; identité internationale d'équipement mobile; identité internationale d'abonné mobile; numéro de carte de module d'identité d'abonné ou numéro de carte SIM);

- adresse(s) de courriel;

- adresses IP;

- identificateur du fournisseur de services locaux, c.-à-d. identification du fournisseur de services de télécommunication à qui appartient le numéro de téléphone ou l'adresse IP dont se sert un client en particulier.

MODÈLE POSSIBLE

Les responsables du dossier examinent soigneusement des options fondées sur un modèle administratif.

MESURES POSSIBLES DE SÉCURITÉ

Conformément aux commentaires reçus à l'issue des consultations tenues en 2002 et en 2005, un certain nombre de mesures de sécurité seraient incluses dans le modèle administratif envisagé, selon lequel les fournisseurs de services de télécommunication seraient tenus de divulguer, à la demande des organismes responsables de l'application de la loi et de la sécurité nationale, des renseignements de base limités sur les noms et adresses des clients. Comme mesures de sécurité, on pourrait :

- établir des restrictions claires concernant le type d'information sur le client qu'il est possible d'obtenir sur demande;

- fixer une limite du nombre d'employés ayant accès à l'information sur les noms et adresses des clients;

- exiger que les personnes ayant accès à l'information soient nommées par les cadres supérieurs de leur organisme;

- exiger que les demandes soient limitées à celles ayant trait à l'exécution d'une tâche ou d'une fonction officielle;

- exiger que ces demandes soient présentées par écrit, à moins de circonstances exceptionnelles;

- exiger que les agents désignés fournissent de l'information connexe avec leur demande, comme la date ou l'heure précise pour une demande concernant une adresse IP;

- exiger des agents désignés qu'ils s'identifient comme agent désigné sur la demande, et qu'ils donnent la tâche ou la fonction à l'origine de la demande;

- empêcher l'organisme demandeur d'utiliser toute information obtenue à une fin connexe ou autre que celle invoquée en vue de son obtention, à moins que la personne visée n'ait accordé son autorisation pour une utilisation supplémentaire;

- exiger que les chefs de l'organisme effectuent régulièrement des vérifications internes afin de veiller à ce que les demandes d'information sur les noms et adresses des clients soient bien conformes aux protocoles et aux mesures de sécurité mis en place;

- transmettre les résultats des vérifications internes aux ministres responsables;

- transmettre les résultats des vérifications au Commissaire à la protection de la vie privée du Canada, au Comité de surveillance des activités de renseignement de sécurité (CSARS) et aux commissaires provinciaux à la protection de la vie privée, s'il y a lieu;

- permettre au Commissaire à la protection de la vie privée du Canada et au CSARS d'effectuer des vérifications ayant trait à la divulgation de l'information sur les noms et adresses des clients;

Aucune des options actuellement en examen n'exige des fournisseurs de services de télécommunication qu'ils effectuent un suivi des actions de leurs clients ou recueillent des données sur ceux-ci sans avoir obtenu les autorisations requises du tribunal gouvernant de telles activités au Canada. De plus, les organismes responsables de l'application de la loi ou de la sécurité nationale ne pourraient pas accéder au contenu des communications d'un client sans avoir l'autorité pertinente.

CONCLUSION

Les responsables planifient de rencontrer les diverses parties intéressées en septembre 2007, afin de discuter les éléments énoncés dans ce document.
Nous vous saurions gré de nous transmettre vos commentaires écrits d'ici le 25 septembre 2007, à l'adresse suivante :

Consultations sur les noms et adresses des clients
Sécurité publique Canada
269, avenue Laurier Ouest, bureau 16C
Ottawa (Ontario) K1A 0P8
Canada

TAB C

Proposed List of Stakeholders for 2007 Consultation

Industry:

- Information Technology Association of Canada (ITAC)
- The Canadian Wireless Telecommunications Association (CWTA)
- Canadian Association of Internet Providers (CAIP)
- David Elder, Bell Canada
- [Industry Canada to propose additional participants]

Consumer/Privacy Advocates/Academics:

- Avner Levin – Ryerson University
- Alicia Wanless – International Perspectives
- Raymond D'Aoust – Office of the Privacy Commissioner
- Canadian Bar Association
- John Boufford – Canadian Information Processing Society
- Paul-Andre Comeau – Professor (ENAP)
- Michael Geist – Professor (University of Ottawa)

Law Enforcement/Victims and Crime Prevention:

- Royal Canadian Mounted Police (National Child Exploitation Co-ordination Centre)
- Canadian Association of Chiefs of Police (Law Amendments Committee)
- Ontario Provincial Police – Project "P"
- Canadian Centre for Child Protection
- Canadian Resource Centre for Victims of Crime
- B'nai Brith

Deacon, James — Amanda, please see comments. 6950-1

From: Deacon, James
Sent: Monday, September 10, 2007 5:11 PM
To: 'Conrad, Alexis: DBR'
Cc: Tait, Amanda; Touizrar, Yacine: PSEPC; Simpson, Richard: ECOM; St. Aubin, Len: DGTP; LePage, Louis: DIF; Hamilton, Jane: ECOM; Noir, Charles: ECOM; Palmer, Philip: LEG; Chatelois, Daniele: ECOM; Evans, Richard
Subject: RE: TALEA - Lawful access / Additional stakeholder list for consultations on Customer Name and Address (CNA)

Thanks for this input.

We agree individual meetings for the larger companies make sense (Rogers, Telus, IBM, Yahoo) to promote ease of discussion.

Will get back to you on the additional additional groups and meetings/new approach you propose. Validation with a final big meeting session is an interesting approach, but not one I am sure we will all be able to execute due to our time frame.

Some stakeholders we have covered in our current list - e.g, office of federal privacy commissioner. Others we do not propose to consult - provincial privacy commissioners, for example - due to time contstraints.

Thanks. We will follow up with you.

Jamie

-----Original Message-----
From: Conrad, Alexis: DBR [mailto:Conrad.Alexis@ic.gc.ca]
Sent: Monday, September 10, 2007 4:50 PM
To: Deacon, James
Cc: Tait, Amanda; Touizrar, Yacine: PSEPC; Simpson, Richard: ECOM; St. Aubin, Len: DGTP; LePage, Louis: DIF; Hamilton, Jane: ECOM; Noir, Charles: ECOM; Palmer, Philip: LEG; Chatelois, Daniele: ECOM
Subject: FW: TALEA - Lawful access / Additional stakeholder list for consultations on Customer Name and Address (CNA)
Importance: High

Jamie,

I am forwarding the message below from Louis, who is out of the office this afternoon. Please let me know if you have any comments or questions.

Best,
Alexis

Alexis Jonathan Conrad
Telecommunications Policy/Politique des télécommunications Industry Canada/Industrie Canada 613.993.0206

==========

Thanks Jamie.

Amanda had proposed an initial list in a previous email. (CWTA, ITAC, CAIP, Bell). I support inclusion of [redacted] (provider of managed services), [redacted], [redacted], [redacted] in the list of stakleholders as proposed in your email.

From my recollection of 2005 consultations, Quebecor (as owners of Videotron) had strong privacy concerns and a fair bit of specific examples. Recommend that we include them in the consultation to ensure that a broad cross-section of views are accounted for.

Based on past interest, you may also wish to include the Canadian Chamber of Commerce, who had co-signed a joint letter to Ms Hurtubise on August 25, 2006 with the other associations.

ask for RCMP/CSIS views

Since the consultation pertains to CNA, I have forwarded the initial consultation plan to my colleagues from the Electronic Commerce team who handle privacy, crypto issues and have responsability for PIPEDA. Follows their suggestions for participants : RIM; (Dave Jaworsky- Director Government & University Relations; Lisa Harder - Government Relations); An instant messenger provider (i.e., Microsoft, Google, or Yahoo!); Crypto providers (i.e. Certicom); Academics, such as Ian Kerr at the University of Ottawa; Appropriate privacy stakeholders (CIPPIC etc.), and provincial privacy commissioners and the federal privacy commissioner.

In my view, stakeholders may not feel at ease to speak freely particularly in regards to specific examples involving their company's experience and process. However, we may wish to benefit from the more dynamic and interactive format of a group meeting.

Therefore, my recommendation would be to hold one meeting with each stakeholder or association, develop a high level summary of the individual consultations and conclude with a final session involving all stakeholders to validate our characterisation of key messages & findings.

Let's discuss if you would consider meeting with the CRTC on matters of access to customer records. In any case, you should be aware that the Commission has an existing regime for access to ALI database which contains confidential subscriber data.

http://www.crtc.gc.ca/archive/ENG/Orders/1998/O98-737.htm
<http://www.crtc.gc.ca/archive/ENG/Orders/1998/O98-737.htm>

http://www.crtc.gc.ca/archive/ENG/Decisions/1999/DT99-17.HTM

Manual Access to the ALI Database

19.As noted, ALI functionality provides the name, telephone number, and service address, whether listed or unlisted, and class of service associated with a 9-1-1 call to the PSAP operator. While the companies' Terms of Service contain provisions with respect to confidential information, the General Tariff Items for 9-1-1 service and the Commission approved standard 9-1-1 agreements between the companies and the municipalities permit the disclosure of confidential customer information on a call-by-call basis solely for the purpose of responding to emergency calls. The General Tariff Items for 9-1-1 service generally provide that the 9-1-1 caller waives the right to privacy to the extent that confidential information in the ALI database is provided to the PSAP.

20.Manual access to the ALI database refers to manual queries of the ALI database for information associated with any telephone number, whether confidential or not. At present, the companies do not permit manual access to the ALI database.

21.The Commission has previously recognized that manual access to the ALI database may be appropriate in certain circumstances. Specifically, in Telecom Order CRTC 98-737 <http://www.crtc.gc.ca/archive/ENG/Orders/1998/O98-737.htm> , 24 July 1998, the Commission approved an agreement between Maritime Tel & Tel Limited and the province of Nova Scotia permitting manual access to the ALI database where a PSAP is unable to identify the location of a person requiring emergency services because the incoming call originates from: (i) a location other than the location requiring emergency services, (ii) a multi-party line, or (iii) a cellular telephone. The Commission notes that if the 9-1-1 caller in such circumstances is aware of the telephone number at the location of the emergency,

Public Safety and Emergency Preparedness Canada | Sécurité publique et Protection civile Canada

File/Docket No. – N° dossier

ACTION REQUEST / FICHE DE SERVICE

To – À: SADMO

Date: Sept. 12, 2007

Purpose/Urgency – But/Urgence

For Signature

Subject/Remarks – Sujet/Remarques

Additional Stakeholders for CNA Consultations

C.C.:
- ☐ Diane MacLaren
- ☐ Chantal Bernier
- ☐ J. Scott Broughton
- ☐ Richard Fiutowski
- ☐ Daniel Lavoie
- ☐ Elisabeth Nadeau

Consultations undertaken / Consultations entreprises :

Legal / Services juridiques _____

Corporate Management / Gestion ministérielle _____

PCO-IGA / BCP-AIG _____

	Name/Signature Nom/Signature	Date
Originator Originateur	Yacine Touzrar	Sept. 12/07
Director/ Chief Directeur/ Chef	James Deacon	
Director General Directeur général	Richard Evans	12-09-07
SADM - SMAS	J. Scott Broughton	
ADM, SPP SMA, PSP		
ADM, CMB SMA, GM		
Comptroller Contrôleur		
ADM, PLEIB SMA, SPALI		
ADM, PRPA SMA, RIPP		
Ministerial Services Division Division des services ministériels		
Deputy Minister Sous-ministre		

PS-51-E (2/05)

Public Safety and Emergency Preparedness Canada
Sécurité publique et Protection civile Canada

MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER

ADDITIONAL STAKEHOLDERS TO TAKE PART IN THE CONSULTATIONS ON THE ACCESS TO CUSTOMER NAME AND ADDRESS (CNA) INFORMATION COMPONENT OF DRAFT LAWFUL ACCESS LEGISLATION

SUMMARY

- You recently signed a set of letters inviting various stakeholders to attend CNA consultations in the coming weeks (see **TAB A** for the list of invitees).

- Following further discussions with Industry and input received on September 10, a number of additional stakeholders are now proposed to be included in the consultations:
  - Rogers
  - Telus
  - Yahoo
  - IBM
  - Videotron
  - Canadian Chamber of Commerce
  - Canadian Internet Policy and Public Interest Clinic (CIPPIC)
  - Federal Ombudsman for Victims of Crime.

- If you agree, consultations with these parties will be scheduled as soon as possible. The target is now to have met with all consultation participants by early October.

- It is recommended that you sign the invitation letters attached (**TAB B**).

James Deacon

Yacine Touizrar (991-1978)

Enclosures: (2)

Stakeholders Attending the Customer Name and Address (CNA) Consultations

Mr. Bernard Amyot
President
Canadian Bar Association
865 Carling Avenue, Suite 500
Ottawa, Ontario K1S 5S8

Signy Arnason
Director, Canadian Centre for Child Protection
615 Academy Road
Winnipeg, Manitoba
R3N 0E7

Mr. Peter Barnes
President and CEO
Canadian Wireless Telecommunications Association
1110-130 Albert Street
Ottawa, Ontario K1P 5G4

Mr. John Boufford
President, Canadian Information Processing Society
5090 Explorer Drive, Suite 801
Mississauga, Ontario L4W 4T9

Mr. Paul-Andre Comeau
Visiting Professor, Canada School of Public Service
373 Sussex Drive
Ottawa, Ontario, Canada
K1N 6Z2

Mr. Tom Copeland
Chair
Canadian Association of Internet Providers
388 Albert Street, 2nd Floor
Ottawa, Ontario K1R 5B2

Mr. Bernard Courtois
President and CEO
Information Technology Association of Canada
220 Laurier Ave. W, Suite 1120
Ottawa, ON K1P 5Z9

Mr. Raymond D'Aoust
Assistant Privacy Commissioner
Office of the Privacy Commissioner of Canada
112 Kent Street, Suite 300
Place de Ville
Ottawa, Ontario K1A 1H3

Mr. David B. Elder
Vice President, Regulatory Law
Bell Canada
110 O'Connor Street, 7th floor
Ottawa, Ontario K1P 1H1

Professor Michael Geist
Canada Research Chair in Internet and E-commerce Law
University of Ottawa, Faculty of Law, Common Law Section
57 Louis Pasteur, Box 450, Stn. A
Ottawa, ON K1N 6N5

Heidi Illingworth
Executive Director, Canadian Resource Centre for Victims of Crime
100 - 141 Catherine Street
Ottawa, ON
K2P 1C3

Mr. Avner Levin
Faculty of Business
Ryerson University
350 Victoria Street
Toronto, Ontario
M5B 2K3

Mr. Michael Mostyn
Director of Government Relations, B'nai Brith Canada
Fuller Bldg. 75 Albert Street
Ottawa, Ontario K1P 5E7

Deputy Commissioner Peter Martin
Royal Canadian Mounted Police
RCMP Headquarters, Nicholson Building
1200 Vanier Parkway, Room G322
K1A 0R2

Deputy Chief Constable Clayton Pecknold and
Assistant Director Pierre-Paul Pichette
Co-Chairs, Law Amendments Committee
Canadian Association of Chiefs of Police
582 Somerset St. W
Ottawa, ON K1R 5K2

Inspector Andy Stewart
Ontario Provincial Police Child Pornography Section
1201 Wilson Ave., Building E, Suite 224
Downsview, Ontario
M3M 1J8

Alicia Wanless
Executive Director, International Perspectives
10 Shallmar Blvd., Suite 1008
Toronto, ON
M5N 1J4
Tel.: (416) 413-1636

Additional Attendees Following Discussion with Industry Canada

Ms. Philippa Lawson
Director, Canadian Internet Policy and Public Interest Clinic
University of Ottawa, Faculty of Law
57 Louis Pasteur St.
Ottawa, ON K1N 6N5

M. Édouard G. Trépanier
Vice-President, Regulatory Affairs, Vidéotron ltée
Champ-de-Mars Building
300 Viger Avenue East
Montréal, Quebec
H2X 3W4

Ms. Asha Gosein
Legal Manager, Yahoo! Canada
106 Front Street East, Suite 200
Toronto, Ontario
M5A 1E1

Mr. Kenneth G. Engelhart
Vice-President – Regulatory
Rogers Communications Inc.
333, Bloor Street East
Toronto, ON M4W 1G9

Mr. Ed Prior
Director, Government & Regulatory Affairs
Telus Mobility
200 Consilium Place, Floor 16
Scarborough, ON M1H 3J3

Mr. Steve Sullivan
Federal Ombudsman for Victims of Crime
240 Sparks St.
P.O. Box 55037
Ottawa, ON
K1P 1A1

Mr. Kim Devooght
VP Public Sector
IBM Canada
2220 Walkley Rd.
Ottawa, ON K1G 5L2

Mr. Michael Murphy
Executive VP Policy
Canadian Chamber of Commerce
360 Albert St., suite 420
Ottawa, ON K1R 7X7

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Mr. Kenneth G. Engelhart
Vice-President – Regulatory
Rogers Communications Inc.
333, Bloor Street East
Toronto, ON M4W 1G9

Dear Mr. Engelhart:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should you have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Canada

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Mr. Ed Prior
Director, Government & Regulatory Affairs
Telus Mobility
200 Consilium Place, Floor 16
Scarborough, ON M1H 3J3

Dear Mr. Prior:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should you have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Canada

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Ms. Asha Gosein
Legal Manager, Yahoo! Canada
106 Front Street East, Suite 200
Toronto, Ontario
M5A 1E1

Dear Ms. Gosein:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should you have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Canada

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Mr. Kim Devooght
VP Public Sector
IBM Canada
2220 Walkley Rd.
Ottawa, ON K1G 5L2

Dear Mr. Devooght:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should you have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Canada

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

M. Édouard Trépanier
Vice-président, affaires réglementaires, Vidéotron ltée
Édifice Champ-de-Mars, 300 avenue Viger est
Montréal (Québec)
H2X 3W4

Monsieur Trépanier,

Sécurité publique Canada aimerait obtenir, au cours des semaines à venir, vos commentaires sur les mesures à prendre pour répondre aux exigences en matière d'accès légal des organismes responsables de l'application de la loi et de la sécurité nationale, relativement aux renseignements sur les noms et adresses des clients que tiennent les fournisseurs des services de télécommunications.

Pour votre examen, vous trouverez ci-joint le document de travail qui servira de base aux discussions. L'accès légal a fait l'objet de deux séances de consultation avec les intervenants en 2002 et 2005. Comme indiqué dans le document ci-joint, les prochaines consultations porteront exclusivement sur les approches qui permettraient aux organismes responsables de l'application de la loi et de la sécurité nationale d'obtenir l'accès nécessaire aux noms et adresses des clients, tout en assurant la protection des renseignements personnels.

Vos commentaires sur toute question relative au document de travail seront les bienvenus. Des téléconférences ou des réunions en personne se tiendront prochainement à Ottawa. Vous pouvez également soumettre vos commentaires par écrit à l'adresse mentionnée dans le document ci-joint. Dans cette éventualité, veuillez transmettre vos commentaires écrits avant le 25 septembre 2007.

Si vous ou votre organisation désirez participer aux consultations, je vous invite à communiquer avec Mme Amanda Tait, agente chargée des politiques, au numéro de téléphone ou à l'adresse électronique suivants : 613 949-3184, Amanda.tait@ps.gc.ca.

Canada

Vous êtes également invité à communiquer avec Mme Tait pour obtenir des renseignements supplémentaires et confirmer votre participation.

Je vous remercie de l'intérêt que vous portez à cette importante question de sécurité publique, et c'est avec plaisir que j'attends vos commentaires.

Veillez agréer mes salutations les plus distinguées.

Lynda Clairmont
Sous-ministre adjoint associée
Secteur de la gestion des mesures d'urgence et sécurité nationale

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Mr. Michael Murphy
Executive VP Policy
Canadian Chamber of Commerce
360 Albert St., suite 420
Ottawa, ON K1R 7X7

Dear Mr. Murphy:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should you have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Ms. Philippa Lawson
Director, Canadian Internet Policy and Public Interest Clinic
University of Ottawa, Faculty of Law
57 Louis Pasteur St.
Ottawa, ON K1N 6N5

Dear Ms. Lawson:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should you have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Canada

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Public Safety Canada
Sécurité publique Canada

Ottawa, Canada
K1A 0P8

Mr. Steve Sullivan
Federal Ombudsman for Victims of Crime
240 Sparks St.
P.O. Box 55037
Ottawa, ON
K1P 1A1

Dear Mr. Sullivan:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Canada

Should you have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Deacon, James

From: Deacon, James
Sent: Tuesday, September 11, 2007 5:00 PM
To: Clairmont, Lynda
Cc: Martel, Kim; Carbino, Michelle
Subject: FW: MLs on lawful access

2007-09-11 ML TALEA and public...

Fyi - media calls today. These are our lines.

Will forward further on this momentarily.

-----Original Message-----
From: Deacon, James
Sent: Tuesday, September 11, 2007 4:43 PM
To: Adamczyk, Aggie
Cc: Evans, Richard; Savoy, Jennifer; 'LePage, Louis: DIF'; McLinton, Philip; Tait, Amanda; Touizrar, Yacine
Subject: FW: MLs on lawful access

Changes to final section - added ref to previous consultations. Took out fierce in front of opponent in lead lines.

Jamie

-----Original Message-----
From: Adamczyk, Aggie
Sent: Tuesday, September 11, 2007 4:27 PM
To: Adamczyk, Aggie; Deacon, James
Cc: 'chris.damico@pco-bcp.gc.ca'; Savoy, Jennifer; Evans, Richard; Tait, Amanda; McLinton, Philip
Subject: MLs on lawful access

Here is the version for NSD DG approval.

Aggie
(613) 949-9738

-----Original Message-----
From: Adamczyk, Aggie
Sent: September 11, 2007 4:21 PM
To: Deacon, James
Cc: 'chris.damico@pco-bcp.gc.ca'; Savoy, Jennifer; Evans, Richard; Tait, Amanda
Subject: RE: QP note on CNA stakeholder consultations

Uno momento - please allow me to input your latest recommendation :o)

Aggie
(613) 949-9738

-----Original Message-----
From: Deacon, James
Sent: September 11, 2007 4:20 PM
To: Adamczyk, Aggie
Cc: 'chris.damico@pco-bcp.gc.ca'; Savoy, Jennifer; Evans, Richard; Tait, Amanda

Subject: RE: QP note on CNA stakeholder consultations

Fine. [illegible]ck for your approval.

Thanks, J

-----Original Message-----
From: Adamczyk, Aggie
Sent: Tuesday, September 11, 2007 4:08 PM
To: Deacon, James
Cc: 'chris.damico@pco-bcp.gc.ca'; Savoy, Jennifer; Evans, Richard; Tait, Amanda
Subject: RE: QP note on CNA stakeholder consultations

Thanks a lot. Jamie, please confirm the following:

a) This is now NSD approved. B) you're sending the documents shared with stakeholders (I assume we can share).

Latest versions attached. One small change:

- The documents were prepared for the purpose of the limited consultations as described. They are not classified and therefore can be shared.

I am now going to reach out to IC, CSIS and RCMP to request that they flag concerns. We need to respond to media enquiry by 5pm today...

Aggie
(613) 949-9738

-----Original Message-----
From: Deacon, James
Sent: September 11, 2007 3:47 PM
To: Adamczyk, Aggie
Cc: 'chris.damico@pco-bcp.gc.ca'; Savoy, Jennifer; Evans, Richard; Tait, Amanda
Subject: FW: QP note on CNA stakeholder consultations

Please see comments. Have discussed with Rick this approach. On document provisoin to reporter, can provide as not classified.

-----Original Message-----
From: Adamczyk, Aggie
Sent: Tuesday, September 11, 2007 3:18 PM
To: Deacon, James; Tait, Amanda; McLinton, Philip
Subject: RE: QP note on CNA stakeholder consultations

Jamie and I just spoke. Here is the latest version. Note that I need to know, and asking for your comment in the section about CTV obtaining the documents from us.

Philip, can you please share with Industry Canada comms and ask for input? Thanks!

Aggie
(613) 949-9738

-----Original Message-----
From: Deacon, James
Sent: September 11, 2007 3:03 PM
To: Adamczyk, Aggie; Tait, Amanda; Evans, Richard
Subject: Re: QP note on CNA stakeholder consultations

Am calling you now

Sent from my BlackBerry Wireless Handheld

----- ginal Message -----
From: Adamczyk, Aggie
To: Deacon, James; Tait, Amanda; Evans, Richard
Sent: Tue Sep 11 14:33:56 2007
Subject: RE: QP note on CNA stakeholder consultations

Sorry, don't know what you mean there...we'll do our best to interpret :o)

Aggie
(613) 949-9738

-----Original Message-----
From: Deacon, James
Sent: September 11, 2007 2:21 PM
To: Adamczyk, Aggie; Tait, Amanda; Evans, Richard
Subject: Re: QP note on CNA stakeholder consultations

I think that we have to say thois is touchin\ b ase. And a fdollow to earlier broader consults opn essen the samew isssues

Amanda plls revciew mls. Tks j

Sent from my BlackBerry Wireless Handheld

----- Original Message -----
From: Adamczyk, Aggie
To: Deacon, James
Sent: Tue Sep 11 12:51:21 2007
Subject: RE: QP note on CNA stakeholder consultations

Hi Jamie,

Here are my draft lines for your initial review. How would we address that we are only consulting with a few stakeholders (as per Geist's allegations)...

Please provide your comments and then I will show to Jen for a quick spin, if necessary and I'll come back for approval.

Please call me if you want to discuss - everything I know now about TALEA, I only learned this morning, so bear with me :o)

Aggie

Aggie

(613) 949-9738

From: Deacon, James
Sent: September 11, 2007 11:02 AM
To: Larose, Suzanne; St.Arneault, Michelle
Cc: Tait, Amanda; Adamczyk, Aggie; Savoy, Jennifer
Subject: FW: QP note on CNA stakeholder consultations

For transmission to SADMO, approved by DG.

Amanda please shaer with IC, RCMP, CSIS and PCO.

J

-----Original Message-----
From: Deacon, James
Sent: Tuesday, September 11, 2007 8:41 AM
To: Evans, Richard
Cc: Tait, Amanda; Adamczyk, Aggie; Savoy, Jennifer
Subject: FW: QP note on CNA stakeholder consultations

Richard, for review/approval please.

Jamie

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

BY FAX (613) 995-1154

September 19, 2007

Honourable Stockwell Day
Minister of Public Safety
House of Commons
Ottawa Ontario K1A 0A6

Dear Minister:

Proposal to expand law enforcement powers to intercept and seize Canadians' electronic communications and personal information—OIPC File No. F02-16763

Media reports last week indicate that you have decided to extend the scope of and time for consultations on the federal government's current proposals for new law enforcement powers in this area. Allow me first to thank you for taking this important step. Appropriate protections for Canadians' internet use information and electronic communications information are critically important to the privacy and liberty of Canadians, making meaningful and public consultation indispensable and very welcome.

You were quoted in the media last week as reassuring Canadians that their personal information would not be subject to disclosure or seizure without prior judicial authorization. Let me congratulate you on taking this position, which is consistent with existing legislative approaches and, more important, aligns with the constitutional protection of Canadians' privacy, without in any way inappropriately hindering legitimate law enforcement investigations.

This said, it appears from the consultation document now on your department's website that the "customer name information" which could be seized without prior judicial authorization will include information that is clearly within Canadian legislative definitions of "personal information" and thus deserves meaningful protection through prior judicial authorization. I therefore assume that your publicly stated position represents an evolution in the thinking from that found in the consultation document. If I am mistaken in this, I would be grateful for clarification from your department.

This issue is of great importance to residents of British Columbia, which is why I have on several occasions made representations to ministers and federal

Mail: PO Box 9038, Stn Prov Govt, Victoria BC V8W 9A4
Location: 3rd Floor, 756 Fort Street, Victoria BC
T. 250 387 5629 F. 250 387 1696
Toll free through *Enquiry BC* 800 663 7867 or 604 660 2421 (Vancouver)
W. www.oipc.bc.ca

government officials and do so now. In view of the contents of the consultation document now on your department's website, I enclose copies of my April 8, 2005 and December 16, 2002 letters on this subject, the thrust of which remains relevant and which I adopt here.

Privacy is a right of fundamental importance to our democratic tradition and government. It should yield to other pressing public interests only where clearly necessary, judged in light of sound evidence of need, and then only to the extent truly required to achieve those other public interest objectives. I urge you to ensure that privacy is not unnecessarily sacrificed in this instance and that meaningful protections are enshrined in our law.

Yours sincerely,

David Loukidelis
Information and Privacy Commissioner
for British Columbia

copies: Jennifer Stoddart
Privacy Commissioner of Canada

Raymond D'Aoust
Assistant Privacy Commissioner of Canada

Suzanne Hurtubise
Deputy Minister

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

BY FAX

April 8, 2005

The Honourable Anne McLellan PC MP
Deputy Prime Minister and Minister of
Public Safety and Emergency Preparedness
House of Commons
Ottawa, Ontario K1A 0A6

The Honourable Irwin Cotler PC MP
Minister of Justice and Attorney General of Canada
House of Commons
Ottawa, Ontario K1A 0A6

The Honourable David Emerson PC MP
Minister of Industry
House of Commons
Ottawa, Ontario K1A 0A6

Comments on 2005 Lawful Access Proposals—OIPC File No. 16763

This letter comments on the lawful access proposals outlined at the March 14, 2005 briefing we received from officials representing your departments and agencies, as well as the Competition Bureau, the RCMP and CSIS.[1]

1.0 SUMMARY

- These proposals appear to be moving ahead with deliberation. I note my ongoing concern that they are moving ahead without the need for new powers having been clearly established. That being said, this letter focuses on offering constructive criticism of specific aspects of the proposals.

- Our criminal law should affirm that, as regards state interception or seizure of email communications, Canadians have a reasonable expectation of privacy in their email.

- The proposed new power for law enforcement officials to compel disclosure of subscriber information without cause and without prior judicial authorization is

Mailing Address: PO Box 9038, Stn Prov Govt, Victoria B.C. V8W 9A4
Location: Third Floor, 756 Fort Street
Telephone: (250) 387-5629 Facsimile: (250) 387-1696
Toll Free enquiries through *Enquiry BC* at (800) 663-7867 or (604) 660-2421 (Vancouver)
website: http//www.oipc.bc.ca

of significant concern. I remain concerned about whether such a new power is truly necessary. Certainly, law enforcement agencies should have the power to compel such information only where the person making the demand has reason to believe the information is necessary for a law enforcement investigation respecting a criminal offence. Further, it should only be possible for specified supervisory officers within a law enforcement agency to authorize compelled production of subscriber information. (Similar restrictions apply under certain US laws to, for example, the FBI.) Last, it should not be possible for any new power to compel production of subscriber information to become a back door route to creating a database of subscribers, a proposal that was raised in 2002 but has not been the subject of public debate and scrutiny in this process.

- The two new proposed production orders raise concerns. As regards the proposed tracking information production order, in the absence of a final, clear, definition of "tracking information", I cannot say with any precision, on the basis of the material provided to me, what all of the privacy concerns associated with tracking orders might be.

- The proposal for a new transmission data production order that would be available applying the lower test of s. 487.013 of the *Criminal Code* is of significant concern. As defined, "transmission data"—essentially, information identifying "the origin, type, direction, date, time, duration, size, destination or termination of a telecommunication"—would disclose a considerable amount of information about an individual's communications. Such data may not include the text or other information intended by the sender to be communicated, but transmission data are not easily separated from such information. The real risk that transmission data would disclose private information requires application of the higher test in s. 487.012, not the lower s. 487.013 test as proposed.

- As for preservation orders, a 15-day interim preservation order should be available without judicial authorization only in exigent circumstances, such as where delay in obtaining judicial authorization would result in the documents or data no longer being available or where there is an imminent risk to life or safety.

- The proposals raise critical questions around oversight and accountability. There should be a strong legislated requirement to provide an annual statistical report to Parliament and to the public respecting use of any subscriber information compulsion powers, production orders and preservation orders (notably 15-day preservation orders). Any suggestion in the briefing materials that information on use of these significant powers should be secret is unacceptable. Existing *Criminal Code* reporting requirements should be adapted to lawful access powers and enhanced to make them, on a Canada-wide basis, timely, consistent and complete. Such a reporting system would afford Parliament an opportunity to monitor implementation of powers to intercept private communications and seize private material and keep

a watching brief on policy implications. Similar requirements and processes exist under many US criminal and national security laws. There is also a clear need for a new body with responsibility for monitoring the use of these powers generally and with the power of review where appropriate. These measures are necessary to ensure the right balance is struck in the aggregate between Canadians' reasonable privacy interests and the public interest in effective law enforcement.

2.0 DISCUSSION

2.1 Background—On December 16, 2002, I wrote to the then Minister of Justice, the Solicitor General and the Minister of Industry and provided specific comments on the Department of Justice's August 2002 lawful access consultation document. That letter voiced my concern about substantive aspects of what was then being proposed and suggested that the need for changes in light of new technologies remained unclear. Last August, I wrote to the federal government again and expressed my continued concern that the need for any changes had not been established. I urged the federal government to proceed with enhanced interception and search powers only if there is clear and compelling evidence for the need to do so.

2.2 Has the Case for Increased Powers Been Made?—My 2002 and 2004 letters on lawful access both questioned whether the need for enhanced interception and search powers has clearly been shown to exist. Most recently, Minister McLellan's December 7, 2004 letter to me declined again to provide evidence of need, saying this would jeopardize law enforcement interests.

The December 2002 submission from the Canadian Association of Chiefs of Police did address the question of justification, but offered only some 39 examples of cases from across Canada in which our laws were said to fail law enforcement needs in the face of new technologies.

These proposals appear to be moving ahead with deliberation. I note my continued concern that they are proceeding without the need for new powers having been clearly established. That being said, this letter focuses on offering constructive criticism of specific aspects of the proposals.

2.3 The Importance of Strong Privacy Protection—The backdrop to my concerns is the constitutional and legislative protections for privacy that exist in Canada. The right to privacy is by no means absolute, but the balance between state interests and individual rights should only favour state interests where a law or other measure has been shown to be clearly necessary and to intrude on individual privacy only to the least extent possible. This is why the *Criminal Code* protects the privacy of personal communications from unwarranted state surveillance and interception. As the Supreme Court of Canada said in *R. v. Duarte*, [1990] 1 S.C.R. 30, at paras. 21 & 22:

> The reason for this protection is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private

> communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. As Douglas J., dissenting in *United States* v. *White*, *supra* [401 U.S. 745 (1971)], put it, at p. 756: "Electronic surveillance is the greatest leveller of human privacy ever known." If the state may arbitrarily record and transmit our private communications, it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime.

2.4 Specific Comments on the Proposals—I will start with a general comment. Your officials told me that the proposals aim to modernize law enforcement agencies' ability to intercept communications and search for evidence in the face of rapidly-changing technologies. The intent, as I understand it, is to focus on the content of communications, not the technology by which they are made. While I support modernization of interception and search laws, my support extends only to proposals that are clearly needed to modernize laws and do so without inappropriately weakening Canadians' privacy rights.

My specific comments on the proposals follow.

Privacy of Canadians' Email Communications

The federal government's 2002 lawful access consultation document cast doubt on whether email should be considered a private communication. My December 2002 submission argued at some length that Canadians' emails should be considered private communications for the purposes of state interception or seizure of emails.

The current proposals discuss this issue and include a possible definition of "private communications". That definition would make a communication private only where it is "made under circumstances in which it is reasonable for a party to the communication to expect that it will not be intercepted by any third party." To be clear, there should be no suggestion that the possibility that a hacker, for example, might surreptitiously intercept someone's personal email means there can be no reasonable expectation of privacy in that email. Surely all Canadians regard letters they send to be private despite the risk that someone will steal them from a mailbox and improperly read them? Such a risk may influence what information is included in private correspondence, but prudence in protecting sensitive information does not mean the correspondence is not a private communication as regards state interception or seizure of the communication.

As I noted in 2002, Canadian and United States courts have accepted that emails carry a reasonable expectation of privacy. Legislative amendments should clearly affirm this.

Compelling Subscriber Information

We were told that law enforcement agencies need to be able to compel telecommunications service providers, including Internet service providers ("TSPs"), to disclose the names and addresses of subscribers to facilitate the detection, investigation and prosecution of crimes. At present, we were told at our briefing, some TSPs will disclose this information on request (often for a fee), while others require a court order. It was argued at the briefing that there is a need for uniformity, certainty and ease of access to this information to enable law enforcement authorities to cope with criminal use of changing technologies.

The proposal, as I understand it, is to authorize law enforcement agencies to, through designated individuals, require a TSP to disclose the name, address and "prescribed identifiers" of any subscriber. The following description of the identifiers that TSPs would have to provide on demand is taken from in slides 33-35 of *Lawful Access Proposals—Proposals with Respect to Compelling Interception Capability and Access to Subscriber Information*:

> The following are the identifiers a TSP would be required to provide to a designated person, on written or oral request, if available:
>
> (a) where the designated person provides a subscriber's name, a TSP would be required to provide the subscriber's address, telephony subscriber service identifier and Internet subscriber service identifier,
>
> (b) where the designated person provides a subscriber's name and a date and time, a TSP would be required to provide the subscriber's dynamic IP address,
>
> (c) where the designated person provides a subscriber's address, a TSP would be required to provide the subscriber's name, telephony subscriber service identifier and Internet subscriber service identifier,
>
> (d) where the designated person provides a subscriber's address and a date and time, a TSP would be required to provide the subscriber's dynamic IP address,
>
> (e) where the designated person provides one or more of the subscriber's telephony subscriber service identifiers, a TSP would be required to provide the subscriber's name, address, and Internet subscriber service identifier,
>
> (f) where the designated person provides one or more of a subscriber's telephony subscriber service identifiers and a date and time, a TSP would be required to provide the subscriber's dynamic IP address,
>
> (g) where the designated person provides one or more of a subscriber's Internet subscriber service identifiers, a TSP would be required to

provide the subscriber's name, address and telephony subscriber service identifier,

(h) where the designated person provides one or more of a subscriber's Internet subscriber service identifiers and a date and time, a TSP would be required to provide the subscriber's dynamic IP address.

A TSP would have 72 hours to comply in ordinary cases and 30 minutes in cases involving threats to national security or other pressing circumstances specified in the proposal.

The over-riding concern with this proposal is that it would empower law enforcement agencies to compel TSPs to identify their customers in ways that will clearly go beyond simple name and address information. No valid comparison can be drawn between subscriber information and name and address information found in telephone books. The above-quoted description of proposed subscriber identifiers makes this clear. For example, a TSP could, under the proposed disclosure requirement, be forced to disclose information that would identify a subscriber as having visited a particular website at a specific time. During our briefing, I asked whether this proposal would, for example, enable police who routinely monitor websites or chat rooms frequented by suspected pedophiles to compel TSPs to identify customers whose computers were used to visit such sites at a specific time.

We were told this was true, but it was suggested this power would only be used for legitimate law enforcement purposes and that misuse would be treated seriously by any police force. It was also said at the briefing that there is no mistaking the nature of pedophile chat rooms, the inference we drew being that only people who intend to do so actually visit such sites or chat rooms. Innocent bystanders, one might infer, need not fear unwarranted scrutiny by law enforcement agencies.

Assurances that public officials only act in good faith are no substitute for the rule of law. Several important changes to this proposal are necessary.

First, the proposed requirement to record a file number or other identifier is no substitute for substantive criteria governing exercise of the power to compel. It should not be possible to compel production of subscriber information unless the information is clearly necessary for a law enforcement investigation respecting a criminal offence. In this respect, I note the assurance on p. 2 of Minister McLellan's December 7, 2004 letter to me that "[p]olice would use these tools to gather information about specific, identified criminal suspects". As it stands, the proposal is devoid of criteria that would statutorily limit exercise of this power to investigation of "criminal suspects".

Second, it should only be possible for specified supervisory officers within a law enforcement agency to compel production of subscriber information. Some law enforcement agencies may balk at this on the ground that it would interfere with

their management of operations, but it is an important point. The assurance at our briefing that, as a practical matter, departments will not give all officers this power is not meaningful. Nor is the assurance that misuse will be punished internally a sufficiently weighty safeguard.

In contending that some restriction on this power is necessary, I note that the power of the Federal Bureau of Investigation ("FBI") under the *Foreign Intelligence Surveillance Act* ("FISA") to issue administrative subpoenas compelling production of certain information for national security and (latterly) criminal investigation purposes is limited under FISA to certain relatively senior agents in each FBI field office. This should be the case respecting subscriber information in light of the fact that it can readily convey information that goes beyond customer identification. It can, for example, disclose an individual's behaviour in visiting websites.

Third, it should not be possible to use subscriber information to indirectly compile surveillance databases respecting user communities or all subscribers to TSP services. The 2002 lawful access consultation document raised the issue of whether a national subscriber database was desirable, as requested by Canada's chiefs of police. As I understand it, this proposal is not on the table at this time. It should be made clear that the power to compel production of subscriber information cannot be used a back door route for individual agencies or the law enforcement community at large to create such databases. Such databases have not been the subject of public debate and scrutiny in this process and, however it is achieved legislatively, such a limitation is clearly needed.

Fourth, the law should require agencies to routinely purge subscriber information in a timely fashion when it is no longer actively being used.

Two subsidiary points are in order regarding the subscriber information proposal. The only safeguard mentioned to us was the proposed requirement to retain records in relation to each request in which law enforcement agencies would have to document the purpose of each request, references to relevant legislation, file identifiers and information about who made the request. This information would have to be retained as required by any statute "relating to the retention of information or any applicable policies". It would also be "made available for appropriate audit and oversight purposes".

First, it is far from clear which federal, provincial or territorial statutes speak meaningfully to retention of law enforcement information of this kind. British Columbia's *Freedom of Information and Protection of Privacy Act* ("FOIPPA"), for example, applies to municipal police forces. Yet it requires only one-year retention of personal information of an individual where that information is used to make a decision directly affecting the individual. Assuming the information in issue is personal information covered by FOIPPA, it is far from clear that, in the present context, the one-year FOIPPA retention period is adequate. If record retention is really intended to be a safeguard, the federal government must do more than refer to undefined statutes "relating to the retention of information or any applicable policies". Meaningful records retention requirements should be legislated.

Second, what does it mean to say this information would be made available "for appropriate audit and oversight purposes"? Who would decide what is an "appropriate" audit or oversight purpose? To whom would the information be disclosed and under what conditions as to use? Would British Columbia's Police Complaints Commissioner, our independent civilian oversight authority, have a right to this information? Would the Commission for Public Complaints Against the RCMP ("RCMP Complaints Commission") have a right to this information? These questions—which are not answered and should be before going further—go to the critical issue of independent oversight, which is addressed below.

New Production Orders

The federal government is proposing to create two new kinds of production orders under the *Criminal Code*—an order for disclosure of "tracking information" and one for disclosure of "transmission data". We were reminded that two new kinds of production order came into force last September, through s. 487.012 and s. 487.013 of the *Criminal Code*, and were told that the same standards for issuance would apply to the proposed two new production orders.

For reasons given below, I have concerns about both of these proposed orders. I will provide some background about the *Criminal Code* provisions cited in the proposals before outlining my concerns.

Section 487.012(1) of the *Criminal Code* authorizes a judge or justice to order a person to produce documents or data, or certified true copies, to a peace officer specified in the order. The order can also require creation of a document based on existing documents. Section 487.012(3) reads as follows:

> (3) Before making an order, the justice or judge must be satisfied, on the basis of an *ex parte* application containing information on oath in writing, that there are reasonable grounds to believe that
>
> (a) an offence against this Act or any other Act of Parliament has been or is suspected to have been committed;
>
> (b) the documents or data will afford evidence respecting the commission of the offence; and
>
> (c) the person who is subject to the order has possession or control of the documents or data.

Section 487.013(1) of the *Criminal Code* reads as follows:

> (1) A justice or judge may order a financial institution, as defined in section 2 of the *Bank Act*, or a person or entity referred to in section 5 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, unless they are under investigation for an offence referred to in paragraph (4)(*a*), to produce in writing the account number of a person named in the order or the name of a person whose account number is specified in the order, the status and type of the account, and the date on which it was opened or closed.

Section 487.013(4) reads as follows:

> (4) Before making an order, the justice or judge must be satisfied, on the basis of an *ex parte* application containing information on oath in writing, that there are reasonable grounds to suspect that
>
> (a) an offence against this Act or any other Act of Parliament has been or will be committed;
>
> (b) the information will assist in the investigation of the offence; and
>
> (c) the institution, person or entity that is subject to the order has possession or control of the information.

We were told the proposal is to allow the new production orders to be issued using the lesser standard of s. 487.013, which requires only "reasonable grounds to suspect" the matters mentioned in s. 487.013(4)(a) through (c).

As regards the proposed tracking information production order, the briefing material says "tracking information" means "information that would assist in determining the location of a person or thing at a particular time". I am aware that s. 487.013(4) applies the same standard of reasonable suspicion as is now found in s. 492.1 of the *Criminal Code*. This is not to say there are no privacy concerns associated with the proposed new tracking information order and, in the absence of a final, clear, definition of "tracking information", I cannot say what other privacy concerns might be associated with tracking information orders.

I have concerns about the proposed transmission data production order. As I understand the proposal, the lower threshold of s. 487.013 is appropriate because, as the briefing material says, transmission data orders would not compel production of "the content of a communication".

The definition of "transmission data" provided to us reads as follows:

> "transmission data" means data relating to the telecommunications functions of dialing, routing, addressing or signaling that identifies or purports to identify the origin, type, direction, date, time, duration, size, destination or termination of a telecommunication generated or received by means of a telecommunications facility.

Data identifying "the origin, type, direction, date, time, duration, size, destination or termination of a telecommunication" can disclose a considerable amount of information about an individual's communications. It may not include the content of a communication, in the sense of the text or other information intended by the sender to be communicated, but transmission data are not easily separated from private information, or content, as generally understood. The real risk that transmission data disclose private information requires application of the higher test in s. 487.012 and I urge you not to proceed with this proposal applying the lower authorization threshold of s. 487.013 of the *Criminal Code*. On this point, let

me repeat what I said at p. 7 of my December 2002 submission regarding a similar proposal in the 2002 lawful access consultation document:

> The reality is that telecommunications-associated data can yield a rich lode of information using data-mining and other techniques to disclose information about the intimate details of Canadians' personal lives. Any analogy between dial-number recorders and telecommunications associated data should be rejected and specific production orders for such data should only be available applying existing *Criminal Code* standards. I also note that, before enactment of s. 492.2 of the *Criminal Code*, the Ontario Court of Appeal ruled that use of dial-number recorders to obtain local call information without prior judicial authorization contravened the *Criminal Code* prohibition against interception of private communications. See *R.* v. *Griffith* (1988), 44 C.C.C. (3d) 63. Canadian courts were not unanimous in this view, but the fact remains that the Ontario Court of Appeal and other courts across the country considered even dial-number recorders to be problematic in the absence of any legislated protections for privacy.

Data Preservation Orders

It is proposed that a peace officer or designated public officer be authorized to order anyone suspected on reasonable grounds to possess or control documents or data that, to quote the material we were given, "will assist in the investigation of an offence" under the *Criminal Code* or another federal Act to "preserve the documents or data for a maximum of 15 days." A longer preservation order could be made by a justice or judge, who can issue the order only where satisfied that that a warrant or order "will be sought" to obtain the documents or data. Neither kind of preservation order would authorize seizure or inspection of the documents or data. A warrant or production order would be required.

The 15-day interim preservation order should be available without judicial authorization only in exigent circumstances, such as cases where delay in obtaining judicial authorization would result in the documents or data no longer being available or where there is an imminent risk to life or safety. This is consistent with my 2002 submission on this point.

Modern Oversight and Accountability Mechanisms Are Needed

As indicated earlier, I raised the need for accountability at our briefing. We were told that protections already exist. Reference was made to legislative standards themselves, judicial involvement in issuance of orders, to Charter protections through the courts, to internal police disciplinary processes and to oversight bodies such as the RCMP Complaints Commission and the Security and Intelligence Review Committee ("SIRC"). Each of these offers some safeguards, but, whether taken alone or together, they do not measure up to the challenges presented by the present proposals.

Indispensable though their role is, judges considering applications for orders under the *Criminal Code* or dealing with Charter challenges are reacting to specific factual circumstances. Each case is only a small part of the overall picture. Questions as to the legitimacy of their doing so aside, it is not possible for the courts to monitor big-picture policy implications, on a national basis, of the impact of lawful access powers. The same observation applies with even more force to internal police disciplinary processes and to complaint investigation bodies such as the RCMP Complaints Commission and SIRC, especially because the remedial powers involved there do not approach those of the courts.

At present, the *Criminal Code* requires the Solicitor General of Canada to report annually to Parliament on interception of communications. Although considerable improvements to this reporting system are needed, it does offer an element of transparency about the state's judicially-authorized interception of private communications and seizure of things. It also offers Parliament some insight into the workings of the system and an opportunity to initiate legislative changes if considered desirable.

Any lawful access amendments should, in light of these concerns, provide for annual reporting respecting use of subscriber information compulsion powers, production orders and preservation orders (notably 15-day preservation orders). Any suggestion in the briefing materials that information on use of these significant powers should be secret is unacceptable. To the contrary, the present *Criminal Code* reporting requirements should be adapted to lawful access powers and enhanced to make them more timely, consistent and complete. Such a system would, again, afford Parliament an opportunity to monitor implementation of these extra-ordinary powers to intercept private communications and seize private material and keep a watching brief on policy implications. Similar requirements and processes exist under many US criminal and national security laws.

There is also a clear need for a new transparency and monitoring framework respecting use of surveillance, interception and communications seizure powers. My colleague, Jennifer Stoddart, Privacy Commissioner of Canada, has made this point in recent months. It is also a point addressed in our October 2004 report, *Privacy and the USA Patriot Act—Implications for British Columbia Public Sector Outsourcing* (found through www.oipc.bc.ca). An ongoing body with responsibility for monitoring use of these powers—and ideally the power to review or investigate specific cases—is desirable in order to ensure the right balance is struck on an ongoing basis between Canadians' reasonable privacy interests and the public interest in effective security and law enforcement.

Media reports of the government's proposed Parliamentary oversight committee offer encouragement on this front and such a body could fulfill some of the functions just mentioned. Further, I understand the Swiss government has, in relation to its lawful access legislation, created an oversight body with policy-related functions, as well as review functions (in addition to the role of Swiss courts in authorizing interception or searches). This example is likely, in my view, to offer useful guidance for Canada as we move forward.

Allow me to extend my sincere thanks for your having sought my office's views on the lawful access proposals and for having consulted stakeholders across Canada. I would be happy to answer any questions you might have.

You should know that I will be posting a copy of this letter on my office's website, at www.oipc.bc.ca.

Yours sincerely,

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia

copies: Sheridan Scott, Commissioner of Competition
Competition Bureau

Margaret Bloodworth, Deputy Minister of Public Safety
and Emergency Preparedness

John H. Sims, Deputy Minister of Justice

Suzanne Hurtubise, Deputy Minister, Industry Canada

Jennifer Stoddart, Privacy Commissioner of Canada

Canadian Privacy Commissioners & Ombudsmen

1 This letter is based on the lawful access proposals as outlined at the March 14, 2005 briefing, which was based on bullet-point PowerPoint slides, copies of which have been provided to us. Specifically, we have received the following PowerPoint materials:

(a) *Combating Cyber-Crime: The Context* (March 2005),
(b) *Lawful Access Proposals—Proposals with Respect to Compelling Interception Capability and Access to Subscriber Information* (March 2005),
(c) *Lawful Access: Legal Review (Follow-up Consultations: Criminal Code Draft Proposals)* (February-March 2005),
(d) *Transmission Data: Considerations for Criminal Law Policy* (February 2005),
(e) *Courriels: Facteurs à considérer en matière de politiques de droit penal* (mars 2005) (and an English translation of this document), and
(f) *Lawful Access—Amendments to the Competition Act* (March 2005).

The comments in this letter are based on the oral briefing and material just described. My office reserves the right to make further comments or adjust the present comments in light of legislative provisions actually tabled in Parliament and in light of any regulations that may be made by Cabinet. For clarity, these comments relate to both the *Criminal Code* and *Competition Act* proposals.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

BY FAX

December 16, 2002

Hon. Martin Cauchon
Minister of Justice and Attorney General of Canada
284 Wellington Street
Ottawa, Ontario K1A 0H8

Hon. Wayne Easter
Solicitor General of Canada
340 Laurier Avenue West
Ottawa, Ontario K1A 0P8

Hon. Allan Rock
Minister of Industry
235 Queen Street
Ottawa, Ontario K1A 0H5

Comments on *Lawful Access – Consultation Document* (August 25, 2002) – OIPC File No. 16763

This letter comments on the above consultation document of the Department of Justice, Industry Canada and the Solicitor General of Canada. That document invites comments on legislative proposals for lawful access by law enforcement agencies to communications and related information.

1.0 SUMMARY

- No evidence has been offered that existing interception and search and seizure laws are inadequate for dealing with electronic communications. Nor does the Cyber-Crime Convention offer a persuasive rationale for the proposals.

- Privacy is a constitutionally protected right. Privacy in electronic communications should give way to law enforcement and national security needs only where those needs clearly outweigh the privacy interest and then only to the minimal extent necessary. There is clearly a reasonable expectation of privacy in e-mail. Existing standards respecting interception of private communications should apply to e-mail interception.

Mailing Address: PO Box 9038, Stn Prov Govt, Victoria B.C. V8W 9A4
Location: Fourth Floor, 1675 Douglas Street
Telephone: (250) 387-5629 Facsimile: (250) 387-1696
Toll Free enquiries through *Enquiry BC* at (800) 663-7867 or (604) 660-2421 (Vancouver)
website: http//www.oipc.bc.ca

- Requiring service providers to acquire the technical capacity to provide lawful access inappropriately co-opts the private sector in state surveillance. The costs to service providers will raise consumer costs and may diminish the competitiveness of the Canadian Internet industry, thus exacerbating concerns about private sector involvement in state surveillance. The development and implementation of Internet technology will be driven by the interests of surveillance and not the needs or realities of Canadian businesses and consumers.

- A specific production order for telecommunications associated data should be available only from a judicial authority applying existing standards and not lower thresholds. Production orders for subscriber or service provider information also should only be available from a judicial authority applying existing standards.

- A data preservation order should be available only from a judicial authority using existing interception standards. Law enforcement authorities should, consistent with s. 487.11 of the *Criminal Code*, only be able to secure preservation when it would be impracticable to obtain a judicial order in the circumstances.

- In the context of creation of a number of surveillance databases in Canada, the proposal of the Canadian Association of Chiefs of Police to create a mandatory-reporting database of all subscribers is worrisome. Final comment is withheld, however, pending further clarification of the proposal and its details.

- Independent oversight of the nature and frequency of use of any new lawful access powers is necessary, recognizing that such oversight must be designed to appropriately protect law enforcement interests.

2.0 DISCUSSION

2.1 Where is the Evidence of Need? – The consultation document says that, for law enforcement and national security agencies, lawful access is an essential tool in the prevention, investigation and prosecution of serious offences and the investigation of security threats. It says telecommunications and computer networks such as the Internet can be used "in the planning, coordination, financing and perpetration of crimes and threats to public safety and the national security of Canada" (p. 3). The paper also says, at p. 3, that

> ... rapidly evolving technologies pose a significant challenge to law enforcement and national security agencies that require lawful access to communications and information, as these technologies can make it more difficult to gather the information required to carry out effective investigations.

The paper contends that, in light of the easy flow of information and communications around the world, law enforcement and national security agencies "need modern and effective capabilities to support their investigative or intelligence gathering efforts" (p. 4). For this reason, the document suggests "partnerships with Canadian industry are more important than ever and must be consistently fostered and maintained" (p. 4).

It is striking that the consultation document offers no evidence to support any suggestion that law enforcement or national security activities have been, or could reasonably be expected to be, impaired because existing laws respecting interception or search and seizure are inadequate given present technologies or trends in communication technologies or information flows. In the absence of any persuasive case, based on concrete evidence, that existing Canadian law is inadequate, I question the need for new laws. I am deeply concerned that – bearing in mind that the lawful access proposals are in various respects rather vague at this stage – the proposals weaken existing legal protections for privacy in Canada without a clear and compelling justification.

The contention that changes in Canadian law are necessary so Canada can ratify the Council of Europe *Convention on Cyber-Crime* ("Cyber-Crime Convention") only goes so far. That treaty is encountering very serious resistance, notably in Europe, because of the serious concerns it raises about individual liberty and privacy and because of concerns about the costs to the private sector of implementing treaty-conformed national laws.

In Australia, for example, the Senate has rejected the *Telecommunications Interception Legislation Amendment Act 2002*. In South Africa, the *Interception and Monitoring Act* was abandoned because of public resistance. In recent weeks, officials of the Home Office in the United Kingdom have conceded that the government must begin again with its implementation of the interception and seizure aspects of the much-criticized *Regulation of Investigatory Powers Act*. Among the few countries to have succeeded in enacting laws or implementing proposals comparable to aspects of the Canadian proposals are China, Iraq and Saudi Arabia.

The Government of Canada should only proceed further with the lawful access proposals if a clear evidentiary basis is offered to support the need for changes. To be sure, the Government of Canada should not proceed simply because it is expedient to do so in the post-September 11 climate of fear and insecurity.

Bearing this overriding reservation in mind, the balance of this letter comments on specific aspects of the proposals assuming, only for the purposes of argument, that a need for them has been established on clear evidence.

2.2 Privacy and Electronic Communications – I will first note the constitutional dimensions of privacy in communications and address privacy in e-mail communications.

Privacy and the Canadian constitution

The constitutional dimensions of the right to privacy are beyond debate. The Supreme Court of Canada has on many occasions affirmed that the *Canadian Charter of Rights and Freedoms* affords constitutional protection for Canadians' privacy. For present purposes, I need only quote from the Court's decision in *R.* v. *Duarte*, [1990] 1 S.C.R. 30, at paras. 21 & 22, which relates to interception of communications:

> The rationale for regulating the power of the state to record communications that their originator expects will not be intercepted by anyone other than the person intended by the originator to receive it (see definition section of Part IV.1 of the

[*Criminal*] *Code*) has nothing to do with protecting individuals from the threat that their interlocutors will divulge communications that are meant to be private. No set of laws could immunize us from that risk. Rather, the regulation of electronic surveillance protects us from a risk of a different order, *i.e.*, not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words.

The reason for this protection is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. As Douglas J., dissenting in *United States* v. *White*, *supra* [401 U.S. 745 (1971)], put it, at p. 756: "Electronic surveillance is the greatest leveller of human privacy ever known." If the state may arbitrarily record and transmit our private communications, it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime.

In debate over anti-terrorist and other measures, I have consistently acknowledged that law enforcement agencies and national security agencies should not be hampered in their law enforcement and national security activities by unwarranted concern for individual privacy rights. The balance between state interest and individual rights should only favour state interests, however, where a law or other measure has been shown to be clearly necessary and to intrude on individual privacy only to the least extent practicable. The existing *Criminal Code* provisions respecting interception of private communications appropriately balance individual privacy interests against the public interest in effective law enforcement.

E-mails are private communications

The consultation paper appears to suggest that e-mails are not private communications. It refers to s. 183 of the *Criminal Code*, which defines "private communication" as including any telecommunication or oral communication made under circumstances creating a reasonable expectation of privacy. The paper suggests that this indicates that a written communication is not a "private communication". The paper refers to decisions by some courts that tape-recorded messages, like written letters, are not "private communications" within the meaning of the *Criminal Code* definition, because it is not reasonable for anyone sending a tape or letter to expect that it will remain completely private.

The consultation paper's appeal to the existing *Criminal Code* definition of "private communication", and to court decisions dealing with it, does not advance the analysis. The question remains, should e-mails be regarded as private communications? The obvious and only answer is that e-mails are private communications. The fact that it may be possible for hackers or others to intercept an e-mail using inappropriate technologies or methods does not undercut this. Surely all Canadians regard letters they send to be

private despite the risk that someone will steal them from a mailbox and improperly read them? Such a risk may influence what information is included in private correspondence, but prudence in protecting sensitive information does not mean the correspondence is not a private communication.

The Alberta Court of Appeal has held that there is a reasonable expectation of privacy in e-mail. See *R.* v. *Weir*, [2001] A.J. 869 (affirming [1998] A.J. No. 155). As the trial judge noted in that case, in *United States* v. *Maxwell*, [1995] 42 M.J. 568, the U.S. Air Force Court of Criminal Appeals held, at p. 576, that e-mails carry an objective expectation of privacy, in the following terms:

> However, we find appellant definitely maintained an objective expectation of privacy in any e-mail transmissions he made so long as they were stored in the America Online computers
>
> In our view, the appellant clearly had an objective expectation of privacy in those messages stored in computers which he alone could retrieve through the use of his own assigned password. Similarly, he had an objective expectation of privacy with regard to messages he transmitted electronically to other subscribers of the service who also had individually assigned passwords. Unlike transmissions by cordless telephones, or calls made to a telephone with six extensions, or telephone calls which may be answered by anyone at the other end of the line, there was virtually no risk that the appellant's computer transmissions would be received by anyone other than the intended recipients.

An e-mail should be explicitly recognized by our criminal law as a private communication and should be protected accordingly. Existing *Criminal Code* interception standards should apply and lower standards for interception of e-mails are not desirable. Many of the weaknesses of consultation paper proposals stem from the apparent assumption that e-mail is not a private communication and does not deserve protection as such. Other flaws in the proposals flow from the similar assumption in the paper that data associated with e-mail traffic, Internet addresses and traffic and other such data do not engage privacy interests because they have little or no privacy content.

2.3 Imposing Lawful Access Capabilities – The consultation document suggests that all wireless, wireline and Internet service providers should be required to ensure that their systems have the technical capacity to provide lawful access to law enforcement and national security agencies. This intercept capability would include content and 'telecommunications associated data' (as the latter term is defined in the document).

The proposal to require Internet service providers to meet certain technical standards amounts to forcing businesses to collect and organize data in a manner that is driven by the need to provide lawful access – in the interests of alleged law enforcement needs and state surveillance – rather than a particular business imperative. This could skew business models and the market, not to mention the impact on consumers.

First, I echo the serious concern voiced around the world that imposition of this capability on service providers inappropriately conscripts the private sector as an agent of the state, not a partner, who engages in surveillance for the state. This point is fundamental. Imposition of a technical intercept capability would greatly blur the line

between surveillance activities of, or on behalf of, the state and commercial surveillance. Creation of a surveillance state is, of course, to be avoided at all costs, but that is precisely the direction in which this proposal tends.

Second, such a proposal carries grave cost implications for service providers, especially Internet service providers. The bursting of the Internet bubble may have set back electronic commerce, but it did not destroy it. Imposition of a costly lawful access capacity requirement will almost certainly further inhibit electronic commerce. Have such risks and benefits of imposing such a lawful access requirement been assessed? In the Netherlands, for example, cost implications for Internet service providers have been so significant that the government has been forced several times to postpone the deadline for compliance with a technical intercept capacity requirement legislated a few years ago. Similar concerns have been expressed, and difficulties encountered, in the United States under the 1996 *Communications Assistance to Law Enforcement Act*. European Union countries have encountered stiff resistance from service providers on this very issue.

While these cost implications do not directly affect privacy interests, I am concerned that the end-result could be to cause consolidation in the Internet service industry. Such a consolidation would reduce competition, could affect service levels and certainly would exacerbate concerns about private sector surveillance on behalf of the state. Moreover, this proposal would amount to state policy regarding law enforcement and surveillance driving development and application of technology, not the market.

2.4 Production Orders – The consultation document indicates that several types of production orders are being considered for enactment: a general production order, a specific production order for traffic data and a specific production order for subscriber or service provider information (or both). By production order, the document means an order that would compel service providers to produce information to law enforcement agents within a set period.

As I understand it, a general production order would be similar to a search warrant, the salient difference being that a production order would require the service provider to deliver documents to a law enforcement agency or make them available to that agency. In the case of a search warrant, of course, law enforcement agents enter relevant premises to find and take away all material covered by the warrant.

The following comments focus on the proposed specific production orders. At the very least, in each instance I believe that existing legal standards must be preserved. No case has been made for lower standards. As regards the paper's reference to "anticipatory orders", the concept is not fleshed out, so I cannot comment.

Specific production orders for telecommunications associated data

The consultation document proposes, at p. 11, that a specific production order should be available "under a lower standard" than existing *Criminal Code* thresholds for telecommunications associated data, supposedly because Internet traffic data is comparable to telephone number records and dial-number recorders.

I strongly disagree with the paper's assumption that there is a lower expectation of privacy in relation to Internet traffic data, comparable to telephone number-related records and dial-number recorder data. The proposed definition of telecommunications associated data would, in the context of e-mail and Internet use, appear to enable law enforcement agents to obtain the following data: e-mail sent-to and received-by addresses; computer IP addresses; data respecting duration of communications; data as to date and time of communications; data about the size of a communication; data disclosing websites visited; and, possibly, data as to e-mail subject line and attachment file names.

By contrast, dial-number recorders merely record identifying information about telephone numbers called from a specific telephone number, not call-content information or other potentially sensitive information of the kinds I have just described. Further, in the case of wireless telephones, which would be covered by the lawful access proposals, unit location information would be in issue, this distinguishing such data from dial-number recorder data.

The reality is that telecommunications associated data can yield a rich lode of information using data-mining and other techniques to disclose information about the intimate details of Canadians' personal lives. Any analogy between dial-number recorders and telecommunications associated data should be rejected and specific production orders for such data should only be available applying existing *Criminal Code* standards. I also note that, before enactment of s. 492.2 of the *Criminal Code*, the Ontario Court of Appeal ruled that use of dial-number recorders to obtain local call information without prior judicial authorization contravened the *Criminal Code* prohibition against interception of private communications. See *R. v. Griffith* (1988), 44 C.C.C. (3d) 63. Canadian courts were not unanimous in this view, but the fact remains that the Ontario Court of Appeal and other courts across the country considered even dial-number recorders to be problematic in the absence of any legislated protections for privacy.

The document also proposes, rather obscurely, that a specific production order should be available under a lower standard for unspecified "other data or information in relation to which there is a lower expectation of privacy" (p. 12). It is not possible to comment usefully on this proposal in the absence of better information as to what is intended.

Production order for subscriber and service provider information

The consultation paper notes that law enforcement authorities must get "some form of court order" to obtain subscriber or service provider information where that information is not voluntarily disclosed to them by its custodian. The paper also acknowledges that basic customer information has traditionally been made available to law enforcement officials. Yet it is suggested that a specific production order could be made available even if no investigation is under way and according to an unspecified lower threshold.

I am concerned that the case for such orders has, again, not been made out. If law enforcement agencies have traditionally been able to get such information it is not clear to me why authority to compel it is needed. Certainly, if custodians have historically delivered such information to law enforcement agencies to assist existing investigations,

I have reservations about allowing compelled disclosure in non-investigative situations. I am, therefore, skeptical about the need for this proposal, at the very least, and would want to see more detail before commenting further.

2.5 Data Preservation Orders – As the consultation document indicates, the Cyber-Crime Convention contemplates a new tool, called a preservation order. Such orders require service providers to retain and preserve data for as long as it takes a law enforcement agency to obtain a warrant to seize the data or a production order requiring its delivery to the agency.

I am not opposed in principle to this proposal. I accept that, because of the nature of electronic data, it may be necessary for law enforcement agencies, in limited cases, to be able to obtain a preservation order to give them time to apply for a warrant or production order from the appropriate judicial authority. The standards to be applied in obtaining such an order from a judicial authority should ideally be comparable to existing standards. The standard of reasonable grounds to believe an offence has been or may be committed may be one approach to examine.

This is not to say that I support the breadth of the proposals found in Articles 16 and 17 of the Cyber-Crime Convention. To the contrary, I believe those articles are excessively broad. I am also concerned that the 90, 120 or 180-day retention periods mentioned in the consultation paper are excessive. If any preservation order provision is enacted, it should apply only to stored computer data (not paper records), it should be available only in the context of an ongoing investigation into a possible violation of a criminal law and preferably should be available only from a judicial authority applying the criteria of reasonable grounds.

As regards exigent circumstances, where not even a preservation order pending warrant can be obtained, law enforcement authorities should at most be empowered to require a service provider to preserve information only where, consistent with s. 487.11 of the *Criminal Code*, obtaining a judicially-issued preservation order "would be impracticable" in the particular circumstances. It is worth underscoring here my concern that no evidence has been presented whatsoever that this or any of the other proposals is needed because existing laws are inadequate.

The fine line between data preservation orders and legislated data retention requirements must be acknowledged. The latter concept is even more troubling, of course, since it entails creation of massive surveillance databases. For example, in the United Kingdom a one-year retention period for data has been imposed. Apart from the civil liberties concerns data retention raises, one wonders about its efficiency or efficacy. The cost implications are enormous. In a December 12, 2002, ZDNet article, America Online is reported as estimating, in testimony before an all-party Parliamentary inquiry in the United Kingdom, that its setup costs alone to comply with United Kingdom law are roughly £30million, with the same again in running costs. That is the cost for just one Internet service provider. The cost implications of data preservation orders also cannot be underestimated, but certainly data retention requirements should be avoided at all costs.

2.6 National Database of Subscriber Information – I have serious reservations about the proposal of the Canadian Association of Chiefs of Police for establishment of a national database of subscriber information. In addition to the concern that this would also conscript the private sector into surveillance, the creation of such a centralized database must be viewed in light of other database proposals either under way or on the table. I refer here, as an example, to the Canada Customs and Revenue Agency's air traveller database, about which I have previously expressed grave concern.

The proliferation of such databases is deeply troubling. Now more than ever such proposals must be subjected to close scrutiny before they proceed. Failing clear evidence that a national database of subscribers is necessary because existing means of collecting subscriber information are inadequate, or that such a database would actually work and not be circumvented by criminals, I believe the proposal should not be pursued at this time. At the very least, if the proposal proceeds, concerns about accountability and independent oversight are critical and must be addressed.

2.7 Accountability – Nowhere does the consultation paper indicate that accountability measures are being contemplated. If new and broader powers are enacted, and I again suggest the case for them has not been made, a system of accountability is needed. This of course cannot be allowed to jeopardize law enforcement or national security interests, but independent oversight of the frequency and nature of use of new powers is necessary. A body such as the Security and Intelligence Review Committee should be considered in relation to any new law enforcement access to e-mail and other electronic communications data, bearing in mind my concern that the case for the proposed powers has not been made.

Yours sincerely,

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia

cc: Lawful Access Consultation
Criminal Law Policy Section
Department of Justice

George Radwanski
Privacy Commissioner of Canada

Provincial & territorial privacy commissioners and ombudsmen

Public Safety Canada | Sécurité publique Canada

Deputy Minister | Sous-ministre

Ottawa, Canada
K1A 0P8

SECRET

DATE: SEP 2 1 2007

6950-1/348649

MEMORANDUM FOR THE MINISTER

CONSULTATIONS ON ACCESS TO CUSTOMER NAME AND ADDRESS INFORMATION

(For Information and Decision)

ISSUE

- Update on the consultation process currently underway on the issue of access to customer name and address (CNA) information.

CURRENT STATUS

- The Department is proceeding with public consultations on the issue of law enforcement and Canadian Security Intelligence Service (CSIS) access to CNA information.

- Officials have started preparations for individual and/or small group consultations with select stakeholders (**TAB A**) including representatives from industry, privacy groups, law enforcement, and victims groups. Invitation letters were sent to these stakeholders in early September 2007, and written comments were requested by September 25, 2007, (this deadline has subsequently been extended to October 12, 2007, to coincide with the deadline for public comments). Meetings or teleconferences are not anticipated in all cases, as some participants have indicated that they will make written submissions.

- The consultation document (**TAB B**) was posted to the Public Safety Canada website on September 13, 2007. The public has been invited to submit their written comments via email or mail, prior to October 12, 2007. To date, the Department has received relatively few on-line submissions (ten in total). A

standard letter thanking individuals for their contribution is being prepared and will be forwarded to you for approval under separate cover.

- Industry Canada, the Royal Canadian Mounted Police (RCMP), and members of your office have requested that additional stakeholders be formally invited to participate in the consultations (**TAB C**). Given that the consultation document has been made public and is accessible on the Department's website, and given the target of a mid-October conclusion of the consultations, officials will contact additional stakeholders directly by telephone to personally invite their input. Meetings will be arranged if requested.

- The Department does not plan to make public any written submissions received or any notes from discussions with consultation participants. However, should an access to information request be made, much of the material may be subject to release; the parties concerned would be consulted, consistent with access to information and privacy legislation.

- In-person consultations with stakeholders will be led by Public Safety Canada at the director level, with additional participation (as necessary) by representatives from Industry Canada, the RCMP, CSIS and Justice Canada to support full and effective discussions of the issues at hand.

NEXT STEPS

- Officials will begin meetings or teleconferences with identified stakeholders early in the week of September 24, 2007, if you agree. A summary of the consultations and input received will be prepared toward the end of October.

- As discussed, meetings are scheduled with senior officials from CSIS and the RCMP to discuss the rationale for access to CNA information and to explore whether additional data are available in this regard.

Suzanne Hurtubise

for

11 OCT 2007

Minister of Public Safety

Enclosures: (3)

TAB A

List of Stakeholders for 2007 Consultation

Industry:

- Information Technology Association of Canada (ITAC)
- The Canadian Wireless Telecommunications Association (CWTA)
- Canadian Association of Internet Providers (CAIP)
- David Elder, Bell Canada

Consumer/Privacy Advocates/Academics:

- Avner Levin – Ryerson University
- Alicia Wanless – International Perspectives
- Raymond D'Aoust – Office of the Privacy Commissioner
- Canadian Bar Association
- John Boufford – Canadian Information Processing Society
- Paul-Andre Comeau – Professor (ENAP)
- Michael Geist – Professor (University of Ottawa)

Law Enforcement/Victims and Crime Prevention:

- Royal Canadian Mounted Police (National Child Exploitation Co-ordination Centre)
- Canadian Association of Chiefs of Police (Law Amendments Committee)
- Ontario Provincial Police – Project "P"
- Cybertip.ca
- Canadian Resource Centre for Victims of Crime
- B'nai Brith

CUSTOMER NAME AND ADDRESS (CNA) INFORMATION CONSULTATION DOCUMENT

INTRODUCTION

Modern telecommunications and computer networks such as the Internet are a great source of economic and social benefits, but they can also be used in the planning, coordination, financing and perpetration of crimes and threats to public safety and the national security of Canada. By extension, the rapidly evolving nature of these technologies can pose a significant challenge to law enforcement and national security officials who are entrusted with combating these threats, and who employ lawful access to communications and information to do so.

The principles and powers of lawful access must be exercised in a manner consistent with the rights and freedoms guaranteed in the *Canadian Charter of Rights and Freedoms* and while adapting to the rapid pace of technological change.

THE CONSULTATION PROCESS

Public Safety Canada, in collaboration with Industry Canada, is presently examining how to address the challenges faced by police, the Canadian Security Intelligence Service (CSIS) and the Competition Bureau when seeking timely access to basic CNA information in a modern telecommunications milieu. This question was previously considered by stakeholders in broader consultation processes on lawful access issues held in 2002 and 2005.

The purpose of this consultation is to provide a range of stakeholders - including police and industry representatives and groups interested in privacy and victims of crime issues - with an opportunity to identify their current views on possible approaches to updating Canada's lawful access provisions as they relate to law enforcement and national security officials' need to gain access to CNA information in the course of their duties. 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.

The objectives of this process are to maintain lawful access for law enforcement and national security agencies in the face of new technologies while preserving and protecting the privacy and other rights and freedoms of all people in Canada. In striving to attain these goals, it is essential to ensure that the competitiveness of Canadian industry is taken into account and that the solutions adopted do not place an unreasonable burden on the Canadian public.

CURRENT CONTEXT

Timely access to CNA information is an important tool used by law enforcement and national security agencies to fulfil their public safety mandates. This type of information can be vital in the context of investigations of online criminal activity, such as child exploitation.

Law enforcement agencies have been experiencing difficulties in consistently obtaining basic CNA information from telecommunications service providers (TSPs). In the absence of explicit legislation, a variety of practices exists among TSPs with respect to the release of basic customer information, e.g., name, address, telephone number, or their Internet equivalents. Some companies provide this information voluntarily, while others require a warrant before providing any information, regardless of its nature or the nature of the situation. 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. This poses a problem in some contexts. For example, law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation. The availability of such building-block information is often the difference between the start and finish of an investigation.

CNA INFORMATION

In the context of options under consideration by Public Safety Canada and its partner departments and agencies, CNA information refers to basic identifiers that would assist law enforcement and national security agencies to determine the identity of a telecommunications service subscriber, if this information was necessary to the performance of their duties.

The scope of CNA information obtained could include the following basic identifiers associated with a particular subscriber:

- name;
- address(es);
- ten-digit telephone numbers (wireline and wireless);
- Cell phone identifiers, e.g., one or more of several unique identifiers associated with a subscriber to a particular telecommunications service (mobile identification number or MIN; electronic serial number or ESN; international mobile equipment or IMEI number; international mobile subscriber identity or IMSI number; subscriber identity module card number of SIM Card Number);
- e-mail address(es);

- IP address; and/or,

- Local Service Provider Identifier, i.e., identification of the TSP that owns the telephone number or IP address used by a specific customer.

POSSIBLE MODEL

Options based on an administrative model are being considered closely by officials.

POSSIBLE SAFEGUARDS

Further to input received during 2002 and 2005 consultations, a number of safeguards could be included under a possible administrative model requiring the release of limited basic CNA information to law enforcement and national security agencies upon request. These could include:

- clear limitations on what customer information could be obtained upon request;

- limiting the number of employees who would have access to CNA;

- requiring that individuals with access be designated by senior officials within their organizations;

- limiting requests to those made for the purpose of performing an official duty or function;

- requiring that requests be made in writing, except in exceptional circumstances;

- requiring that designated officials provide associated information with their request, e.g., identification of a specific date and time for a request relating to an IP address;

- requiring designated officials to record their status as such when making a request, as well as the duty or function for which a particular request is made;

- limiting the use of any information obtained to the agency that obtained it for the purpose for which the information was obtained, or for a use consistent with that purpose, unless permission is granted by the individual to whom it relates;

- requiring regular internal audits by agency heads to ensure that any requests for CNA information are being made in accordance with the protocols and safeguards in place;

- reporting to responsible ministers on the result of any internal audits;

- provision of any audit results to the Privacy Commissioner of Canada, the Security Intelligence Review Committee, or provincial privacy commissioners, as appropriate;

- provision for the Privacy Commissioner and SIRC to conduct audits related to the release of CNA information.

Under no option being examined would TSPs be compelled to track the actions of customers or to collect information about them in the absence of necessary court authorizations governing such activity in Canada, nor would law enforcement or national security agencies be permitted to obtain the content of a customer's communications without such authorizations.

CONCLUSION

Officials plan to meet with a range of interested parties in September, 2007 to discuss the issues raised in this paper.

Written comments may also be sent to the following address by September 25, 2007, and will be gratefully received:

Customer Name and Address Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON, Canada K1A 0P8

INFORMATION SUR LES NOMS ET ADRESSES DES CLIENTS DOCUMENT DE CONSULTATION

INTRODUCTION

Les nouveaux systèmes de télécommunications et réseaux informatiques comme Internet génèrent d'importants avantages économiques et sociaux. Par contre, ils peuvent également servir à planifier, à coordonner, à financer et à commettre des crimes ainsi qu'à menacer la sécurité publique et nationale du Canada. En raison de leur évolution rapide, ces technologies peuvent causer d'importants problèmes aux responsables de l'application de la loi et de la sécurité nationale qui doivent lutter contre ces menaces et qui, pour se faire, doivent appliquer les principes de l'accès légal aux communications et à l'information.

Les principes et les pouvoirs relatifs à l'accès légal doivent être exercés de façon à respecter les droits et les libertés garantis par la Chartre canadienne des droits et libertés, tout en étant adaptés au rythme rapide de l'évolution des technologies.

LE PROCESSUS DE CONSULTATION

Sécurité publique Canada, en collaboration avec Industrie Canada, examine présentement comment les services de police, le Service canadien du renseignement de sécurité (SCRS) et le Bureau de la concurrence peuvent surmonter les difficultés auxquelles ils doivent faire face lorsqu'ils doivent obtenir de l'information de base sur les noms et adresses des clients, dans le contexte des technologies modernes des télécommunications. Cette question a déjà fait l'objet d'un examen des intervenants, dans le cadre de processus de consultations plus vastes sur l'accès légal, tenues en 2002 et en 2005.

Ces consultations ont pour but de permettre à une vaste gamme de parties intéressées, comme les services de police, l'industrie ainsi que les organismes de défense des libertés civiles et des victimes de crime, de donner leur point de vue sur les démarches possibles qui visent la mise à jour des dispositions canadiennes en matière d'accès légal, en ce qui concerne la nécessité des responsables de l'application de la loi et de la sécurité nationale d'obtenir de l'information sur les noms et adresses des clients dans le cadre de leurs tâches quotidiennes. L'étendue possible de l'information sur les noms et adresses des clients à obtenir est expliquée dans ce document de consultation, mais il faut préciser dès le départ que cette information ne comprendrait d'aucune façon le contenu des communications des clients ou les sites Internet qu'ils ont consultés.

Les objectifs de ce processus visent à maintenir l'accès légal pour les organismes responsables de l'application de la loi et de la sécurité nationale dans le contexte du développement constant de nouvelles technologies, tout en préservant et en assurant la protection de la vie privée ainsi que les autres droits et libertés de toutes les personnes habitant au Canada. La réalisation de ces objectifs doit absolument prendre en compte le fait que l'industrie canadienne doit demeurer concurrentielle et que les solutions adoptées ne doivent pas représenter un fardeau déraisonnable pour le public canadien.

CONTEXTE ACTUEL

L'accès rapide à l'information sur les noms et adresses des clients est un outil important dont se servent les organismes chargés de l'application de la loi et de la sécurité nationale pour s'acquitter de leur mandat touchant la sécurité publique. Lorsqu'il est question d'enquêtes portant sur des cybercrimes, tel que l'exploitation des enfants, ce type d'information peut s'avérer vital.

Il est difficile pour les organismes d'application de la loi d'obtenir des fournisseurs de services de télécommunication, de façon constante, l'information de base sur les noms et adresses des clients. Sans dispositions législatives explicites, les différents fournisseurs de services de télécommunication observent toute une gamme de pratiques en ce qui a trait à la divulgation de l'information de base sur le client, notamment le nom, l'adresse, le numéro de téléphone ou leurs équivalents sur Internet. Certaines entreprises divulguent volontairement cette information, alors que d'autres exigent qu'un mandat soit présenté avant de fournir l'information demandée, quelle que soit la nature de cette information ou le contexte entourant la demande. Si le gardien de l'information refuse de coopérer lorsqu'une demande est faite pour obtenir cette information, les organismes chargés de faire appliquer la loi n'ont aucun moyen d'exiger la production des renseignements relatifs au client, ce qui peut poser problème dans certains cas. Par exemple, les organismes d'application de la loi peuvent avoir besoin de l'information pour des raisons non reliées à une enquête (c.-à-d. pour trouver le plus proche parent en cas d'urgence) ou parce qu'il s'agit d'un début d'enquête. Le fait d'avoir accès à cette information de base constitue souvent la différence entre le début d'une enquête ou sa fin.

INFORMATION SUR LES NOMS ET ADRESSES DES CLIENTS

Dans le contexte des options examinées par les représentants de Sécurité publique Canada et des ministères et organismes partenaires, l'information sur les noms et adresses des clients renvoie aux identificateurs de base qui pourraient aider les organismes responsables de l'application de la loi et de la sécurité nationale à déterminer l'identité d'un abonné d'un service de télécommunication, si cette information était nécessaire à l'exécution de leurs fonctions.

L'information obtenue sur les noms et adresses d'un abonné d'un service de télécommunication en particulier pourrait comprendre les identificateurs de base suivants:

- nom;
- adresse(s);
- numéro de téléphone de dix chiffres (service conventionnel à fil ou service sans fil);

- identificateurs de téléphone cellulaire, c.-à-d. un ou plusieurs identificateurs uniques associés à un abonné d'un service particulier de télécommunication (numéro d'identification de service mobile; numéro de série électronique; identité internationale d'équipement mobile; identité internationale d'abonné mobile; numéro de carte de module d'identité d'abonné ou numéro de carte SIM);

- adresse(s) de courriel;

- adresses IP;

- identificateur du fournisseur de services locaux, c.-à-d. identification du fournisseur de services de télécommunication à qui appartient le numéro de téléphone ou l'adresse IP dont se sert un client en particulier.

MODÈLE POSSIBLE

Les responsables du dossier examinent soigneusement des options fondées sur un modèle administratif.

MESURES POSSIBLES DE SÉCURITÉ

Conformément aux commentaires reçus à l'issue des consultations tenues en 2002 et en 2005, un certain nombre de mesures de sécurité seraient incluses dans le modèle administratif envisagé, selon lequel les fournisseurs de services de télécommunication seraient tenus de divulguer, à la demande des organismes responsables de l'application de la loi et de la sécurité nationale, des renseignements de base limités sur les noms et adresses des clients. Comme mesures de sécurité, on pourrait :

- établir des restrictions claires concernant le type d'information sur le client qu'il est possible d'obtenir sur demande;

- fixer une limite du nombre d'employés ayant accès à l'information sur les noms et adresses des clients;

- exiger que les personnes ayant accès à l'information soient nommées par les cadres supérieurs de leur organisme;

- exiger que les demandes soient limitées à celles ayant trait à l'exécution d'une tâche ou d'une fonction officielle;

- exiger que ces demandes soient présentées par écrit, à moins de circonstances exceptionnelles;

- exiger que les agents désignés fournissent de l'information connexe avec leur demande, comme la date ou l'heure précise pour une demande concernant une adresse IP;

- exiger des agents désignés qu'ils s'identifient comme agent désigné sur la demande, et qu'ils donnent la tâche ou la fonction à l'origine de la demande;

- empêcher l'organisme demandeur d'utiliser toute information obtenue à une fin connexe ou autre que celle invoquée en vue de son obtention, à moins que la personne visée n'ait accordé son autorisation pour une utilisation supplémentaire;

- exiger que les chefs de l'organisme effectuent régulièrement des vérifications internes afin de veiller à ce que les demandes d'information sur les noms et adresses des clients soient bien conformes aux protocoles et aux mesures de sécurité mis en place;

- transmettre les résultats des vérifications internes aux ministres responsables;

- transmettre les résultats des vérifications au Commissaire à la protection de la vie privée du Canada, au Comité de surveillance des activités de renseignement de sécurité (CSARS) et aux commissaires provinciaux à la protection de la vie privée, s'il y a lieu;

- permettre au Commissaire à la protection de la vie privée du Canada et au CSARS d'effectuer des vérifications ayant trait à la divulgation de l'information sur les noms et adresses des clients;

Aucune des options actuellement en examen n'exige des fournisseurs de services de télécommunication qu'ils effectuent un suivi des actions de leurs clients ou recueillent des données sur ceux-ci sans avoir obtenu les autorisations requises du tribunal gouvernant de telles activités au Canada. De plus, les organismes responsables de l'application de la loi ou de la sécurité nationale ne pourraient pas accéder au contenu des communications d'un client sans avoir l'autorité pertinente.

CONCLUSION

Les responsables planifient de rencontrer les diverses parties intéressées en septembre 2007, afin de discuter les éléments énoncés dans ce document. Nous vous saurions gré de nous transmettre vos commentaires écrits d'ici le 25 septembre 2007, à l'adresse suivante :

Consultations sur les noms et adresses des clients
Sécurité publique Canada
269, avenue Laurier Ouest, bureau 16C
Ottawa (Ontario) K1A 0P8
Canada

TAB C

List of Proposed Additional Stakeholders

Industry:

- Rogers
- Telus
- Videotron
- Yahoo Canada
- IBM
- Canadian Chamber of Commerce
- Electro-Federation of Canada

Consumer/Privacy Advocates/Academics:

- Canadian Internet Policy and Public Interest Clinic (CIPPIC)

Law Enforcement/Victims and Crime Prevention:

- Federal Ombudsman for Victims of Crime - Steve Sullivan

Secret

Lawful Access

Briefing for the Minister of Public Safety

September 14, 2007

Lawful Access Proposal

Lawful access proposal has 2 components :

A) Requiring telecommunications service providers to implement and maintain systems that are intercept-capable; and

B) Ensuring timely access to basic customer name and address (CNA) information

Interception Component

- Currently communications service providers are not required to build interception capability into existing or new networks:
  - Police and CSIS may not be able to intercept communications even when a warrant has been obtained
- Currently, Government must negotiate with, and pay, service providers to create interception solutions for networks (e.g. Rogers, Telus, Bell)
  - can take years, with a high-cost to retrofit existing systems
  - some providers refuse to cooperate, or charge a premium for assistance
- Criminals and terrorists are very aware of gaps and exploit them
- New technologies increase gaps

CNA Component

- CNA information is basic identifying information, such as:
  - Name and address;
  - Telephone number;
  - Cell phone identifiers; and
  - Email and Internet Protocol (IP) addresses

- If police and CSIS want more than basic identifying information, they must obtain a warrant

- Police can get CNA on a voluntary basis from some TSPs
  - But many demand judicial authorization before they will provide requested information – and regardless of the nature of the situation (e.g., even in child pornography cases)

- Results in an inconsistent, ad-hoc approach – confusion and uncertainty among all parties

[redacted]

Not relevant

[redacted]

Not relevant

Secret

[redacted]

Past Consultations

- Lawful access the subject of two rounds of broad-based consultations in 2002 and 2005; additional, more limited discussions held with select industry and police representatives in 2006/2007

<u>2002</u>

- Over 20 meetings with a broad range of stakeholders across the country (e.g. industry, privacy, law enforcement/victims groups)
- Public consultation document posted on Justice Canada's web site
- Over 300 written submissions received; summary released to the public in August 2003
- [redacted] Not relevant

Past Consultations (cont.)

2005

- In-depth consultations held with approximately 30 stakeholders (i.e. industry, privacy and law enforcement/victims groups)
- [redacted]
- Following consultations, CNA proposals were amended to increase number of safeguards, as recommended by privacy advocates

2006/2007

- Further limited discussions with industry and police associations
- [redacted]

Proposed Consultation

- Following discussions with Minister of Industry and concerns raised regarding CNA issue, targeted consultation strategy developed
- Scope limited to CNA component
- Targeted initially to a representative selection of stakeholders (industry, privacy, law enforcement/victims groups)
  - Consultation package mailed out (invitation letter and 4-page consultation document containing basic facts)
  - Individual and small group consultations now scheduled to begin week of September 24th
  - Additional names were provided by Minister's Office
- Consultation document posted to Public Safety web site on September 13th; public and organizations invited to provide written comments by October 9th
- Consultations targeted to be complete by mid-October

Possible New Consultation Strategy

1. Increase number of stakeholders

2. Include victim and police representatives

3. Develop communications strategy to support consultations

4. Round-table format

Considerations

NOT RELEVANT/ NON PERTINENT

1.

2.

3.

Protected

Status Report on Customer Name and Address Information Consultations

October 2007

Presentation to the Minister of Public Safety

Public Safety Canada
Sécurité publique Canada

Canada

Consultations Objective and Scope

- Objective: obtain current views on the question of police and CSIS access to CNA information and possible approaches

- Consultations took place in September and early October
  - consultation document posted on Public Safety website in early September

- Selected groups and individuals invited to participate in meetings and/or make submissions
  - representatives of law enforcement, victims groups, privacy stakeholders, and the telecommunications industry

- Public invited to participate by letter or via the Public Safety website
  - deadline for input October 12th

Participation

Invited Groups/Individuals

- 27 groups/individuals were invited to participate in meetings and/or make written submissions
  - e.g., Telus, Bell, Information Technology Association of Canada, Canadian Resource Centre for Victims of Crime, Office of the Privacy Commissioner, National Child Exploitation Coordination Centre/RCMP
- 16 of the invited groups/individuals did participate in meetings or teleconferences
  - some of these have also provided written input
- 3 groups/individual have provided written input only (Canadian Bar Association, Canadian Internet Policy and Public Interest Clinic, Prof. Avner Levin)
  - Still awaiting written submissions from 3 groups
- 5 invitees decided not to participate

Participation (cont'd)

Letters and Emails

- 22 letters to the Minister received to date
  - 19 from private individuals
  - 3 from institutions or representatives (i.e., the Ontario and B.C. privacy commissioners, one Member of Parliament)

- 19 emails received on the Public Safety website
  - 15 from private individuals
  - 4 from interested groups that had not been invited to meetings (e.g. B.C Civil Liberties Association)

Key Input Received

Industry Representatives

- Service providers are willing to help law enforcement and CSIS when there is a need (e.g., child exploitation, national security, urgent circumstances)
- Any compliance requirements in legislation or regulations must be specific and clear to facilitate cooperation and business planning (e.g., timelines for providing information)
- Service providers must be compensated for providing CNA – must recognize that the impact on smaller providers may be great
- There should be no new client information collection or data retention requirements
- Might consider defining specific circumstances in law where information can be accessed (e.g., emergency situations, next of kin notification, child sexual exploitation, national security – any clearly justifiable areas)
  - Is PIPEDA the vehicle to do this?

Key Input Received (cont'd)

Privacy Stakeholders

- Evidence demonstrating the necessity for access to CNA is lacking or absent
- Personal information should not be accessed without judicial authorization – all personal information may be sensitive in certain circumstances
  - PIPEDA needs to be clarified in terms of its allowing companies to provide information where there is "lawful authority"
- Concerned about the potential for abuse of access to CNA, even with administrative safeguards
  - some types of information are more sensitive than others (e.g., Internet and email addresses which may indicate personal activities or preferences)
- Might consider defining specific circumstances where information can be accessed (e.g., emergency situations, next of kin notification, child sexual exploitation, national security - any clearly justifiable areas)

Key Input Received (cont'd)

Victims' Groups

- The reluctance of service providers to assist police is a serious public safety and victim issue
  - this information essential to combating child exploitation and other crimes
- Violation of victims' privacy is the most pressing privacy concern at this time (e.g., child exploitation victims' images are on line)
  - Child victims are getting younger (20% now under 3 years old)
- Impacts on victims are increasing with crimes on-line like ID theft and frauds/scams
- Most in the public would be surprised if police could not access CNA without a warrant
  - Police routinely access this kind of information in other contexts

Key Input Received (cont'd)

Law Enforcement

- Relationships are generally good with service providers (especially the major ones), but growing concerns over level of cooperation in many cases, even in cases of child sexual exploitation
  - Some smaller service providers cater to criminal activity and/or advertise privacy protections (e.g., agree to destroy their files if police call)
- CNA information is vital to initiate investigations in many cases
  - especially in international cases, where often only an Internet address is available as the first lead
- A warrant regime for CNA is untenable – this information is used in early investigation stages, and warrant thresholds could not be met; obtaining court authorizations often takes too long
- There is a limited or no expectation of privacy on basic customer information – police routinely access this kind of information in many other contexts without a warrant (e.g. driver licence checks)

Key Input Received (cont'd)

General Public

- Justification for on-request access by police/CSIS is not clear – is there evidence of a problem?
- Overwhelmingly against access to personal information, particularly email and Internet addresses, without judicial authorization
  - some incorrectly assumed that a warrant is required in all cases today
- Worried about the potential for abuse and "fishing expeditions" by agencies
  - some references to information sharing concerns in the Arar and Air India cases, and to current U.S. practices/laws

Current Status

- Consultations are considered concluded

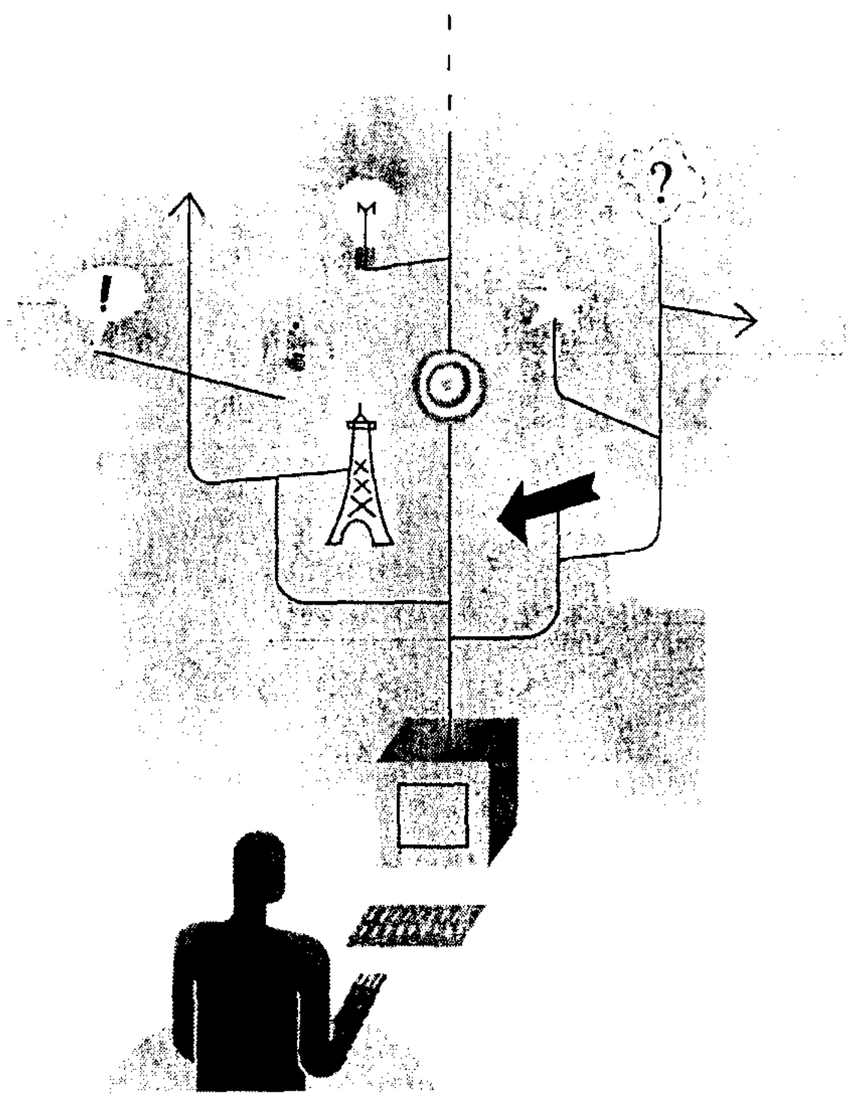
- Summary of consultations being written
  - any further input received will be examined and reflected
  - could post the summary on the departmental website

- Responding to a limited number of media enquiries as to status of consultations and availability of submissions received

ITAC
INFORMATION TECHNOLOGY ASSOCIATION OF CANADA

ACTI
ASSOCIATION CANADIENNE DE LA TECHNOLOGIE DE L'INFORMATION

Customer Name and Address Consultation



October 2007

ITAC is the voice of the Canadian information and communications technologies industry in all sectors, including telecommunication and internet services, consulting services, hardware, microelectronics, software and electronic content. ITAC's network of companies accounts for more than 70 per cent of the 579,000 jobs, $137.6 billion in revenue, $5.2 billion in R&D investment, $22.6 billion in exports and $11.5 billion in capital expenditures that the industry contributes annually to the Canadian economy.

The Information Technology Association of Canada (ITAC) is pleased to respond to Public Safety Canada's discussion paper on customer name and address (CNA) information. The association has been actively involved in government consultations on lawful access to electronic communications since 2002.

Canada's telecom industry has a long history of working cooperatively with law enforcement within Canada's legal framework for lawful access, including access to customer information. All telecommunication service providers (TSPs) have developed some capability of responding to requests from law-enforcement agencies (LEAs) on a routine basis, and generally maintain dedicated security departments whose sole purpose is to respond to such requests and to comply with court orders. These services are provided at considerable cost to the TSPs.

Personal information associated with customers and subscribers of all telecom and internet services offered in Canada is subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which allows TSPs to release a subscriber's personal information when compelled by law to do so. TSPs are also subject to CRTC rules regarding the protection of CNA information, although the specific rules vary among service types. In general, subscriber identifiers – aside from wireline telephone numbers – are expected to be treated as confidential and may be released only when TSPs are compelled by law to do so.

In order to comply with these rules regarding the protection of customer privacy, TSPs currently require a warrant or court order before providing LEAs with confidential customer information except in the most exigent circumstances. The discussion paper appears to suggest that Public Safety Canada is contemplating changes in the scope of CNA information and the circumstances and conditions under which TSPs would be compelled to collect certain specified CNA information and provide it LEAs. TSP obligations must be clearly set out in any new legislation or regulation, but as it is not clear to ITAC what exactly is under consideration we cannot respond in a more detailed fashion at this point.

As mentioned above, TSPs incur significant costs in responding to requests and providing lawful-access services to LEAs, and it is imperative that they be compensated for those costs. Industry concerns will only be exacerbated by a move to a "no warrant" regime – as raised in the discussion paper. The volume of requests for CNA information can be expected to increase substantially absent judicial oversight, with a corresponding substantial increase in costs to TSPs.

With respect to the specific kinds of CNA information, much of the wireline and wireless CNA information listed in the discussion paper is already available either publicly or via CRTC tariffed services. A variety of third parties provide "reverse look-up" services for Canadian telephone numbers and many of these are provided free of charge on the public internet. However, ITAC notes that the "basic identifiers" listed in the discussion paper go well beyond what most people would consider to be basic. IP addresses,

email addresses, IMSIs, ESNs, IMEIs and SIM numbers are not the "tombstone" data that is usually associated with CNA information. Nevertheless, ITAC is not aware of LEAs being unable to obtain the CNA information they require.

Any move to impose new requirements must take into account the fact that TSPs cannot always respond as quickly as may be desired. (For example, systems that provide quick response for directory assistance have not been developed for services other than wireline telephony.) Furthermore, while TSPs work diligently to respond to LEA requests, their ability to provide information is often constrained as a result of the volume of requests, the amount of detail required or other factors such as requests involving historical usage.

ITAC also notes that TSPs do not always have business reasons to collect CNA information, and so may not have in their possession the information sought by LEAs. ITAC would oppose the imposition of an obligation on TSPs to collect information that they would not be collecting for their own purposes. Significant service, business and cost issues would arise if carriers were required to collect, validate and maintain accurate CNA information simply for the purposes of lawful access.

In closing, ITAC acknowledges that lawful access and the ability to obtain CNA information are important tools for LEAs in their efforts to protect society. In its interventions on this issue, ITAC has consistently advocated for standards-based technical requirements, appropriate compensation for TSP costs and a phased-in approach to new obligations.

ITAC will not be able to support efforts to move ahead on this issue if our fundamental concerns continue to be left unaddressed – as they were in the previous legislative proposal, the *Modernization of Investigative Techniques Act*. To function properly, the Canadian lawful-access regime must recognise the realities of the telecommunication industry:

- TSPs must be compensated for the significant costs incurred responding to the requirements of LEAs.
- Any new technical requirements must be based on international standards, and provide an adequate phase-in period.
- The scope of CNA information and the circumstances under which it is to be provided by TSPs to LEAs must be explicitly identified and clarified in any new legislation or regulations.
- CNA information requirements must be applied in a technologically and competitively neutral fashion.
- TSPs must not be required to collect customer information beyond what is already collected for business purposes.

ITAC appreciates the opportunity to share these comments and looks forward to the opportunity to comment on any specific legislative or regulatory amendments that are subsequently developed for consideration, especially if they go beyond the parameters of this consultation. We will of course also be pleased to meet with Public Safety Canada officials to discuss these issues.

As these matters are of considerable importance to Canadians, ITAC suggests that all written submissions to this public consultation be made available for public review on the Public Safety Canada website.

Response of the Office of the Privacy Commissioner of Canada to the Customer Name and Address (CNA) Information Consultation Document

October 2007

The Rationale for the Consultation

According to the consultation document issued by Public Safety Canada and Industry Canada, "The objectives of this process are to maintain lawful access for law enforcement and national security agencies in the face of new technologies while preserving and protecting the privacy and other rights and freedoms of all people in Canada."[1]

The consultation document is based on the assumption that law enforcement and national security (LE/NS) agencies are experiencing difficulties obtaining access to customer name and address (CNA) information in a timely way. The consultation document sets out the problem as follows:

> Law enforcement agencies have been experiencing difficulties in consistently obtaining basic CNA information from telecommunications service providers (TSPs). In the absence of explicit legislation, a variety of practices exists among TSPs with respect to the release of basic customer information, e.g., name, address, telephone number, or their Internet equivalents. Some companies provide this information voluntarily, while others require a warrant before providing any information, regardless of its nature or the nature of the situation. 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. This poses a problem in some contexts. For example, law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation. The availability of such building-block information is often the difference between the start and finish of an investigation.

The excerpt above suggests that the problem is one of inconsistency; some TSPs provide this information voluntarily while others are unwilling to provide this information or will do so only in response to a warrant.

The consultation document states "This poses a problem in some contexts" and it goes on to refer to two situations where problems arise. The first involves the use of CNA information for non-investigative emergency purposes; the second involves the use of CNA information during the early stages of an investigation.

---

[1] The consultation document is available at http://securitepublique.gc.ca/prg/ns/cna-en.asp

Unfortunately the consultation document does not provide any sense of the scope of the difficulties mentioned in the document. Are 80 per cent of TSPs providing CNA information voluntarily or is the figure 20 per cent? Are telephone companies more likely to provide the information than Internet service providers (ISPs)? Are small TSPs more likely to request a warrant? Nor does the consultation document indicate whether TSPs respond differently depending on the situation. For example, do TSPs respond differently to next-of-kin emergency situations than they do to requests involving suspected violent crimes?

Requiring all TSPs to disclose CNA information on request is an overly broad, one size fits all response to a problem that has not been clearly defined or measured. We raised this issue in response to the 2002 consultation and the 2005 consultation on lawful access:

> When the 2002 Consultation Paper on Lawful Access was issued by the Department of Justice, Industry Canada and the Solicitor General, our Office, along with several other parties, questioned the need to revise the existing lawful access regime. We pointed out that the departments had failed to demonstrate the existence of a serious problem that needed to be addressed. We urged the three departments to present a clear statement of the problems that law enforcement agencies were encountering along with empirical evidence supporting the need for enhanced surveillance powers proposed in the consultation paper.
>
> This has still not been done. Without a clear understanding of the problems that the proposed legislation is intended to correct it is impossible for our Office or the Canadian public to determine if the measures being proposed are necessary and proportionate.

Although the current consultation addresses only some of the issues raised in previous consultations, the comments we made in 2005 are still appropriate.

The *Personal Information Protection and Electronic Documents Act (PIPEDA)*

As federal works, undertakings and businesses (FWUBs) all TSPs operating in Canada are subject to *PIPEDA* even if they only provide service in a province with substantially similar legislation.

PIPEDA requires that organizations obtain consent for disclosures of personal information subject to a limited number of exceptions. Three of the exceptions are particularly relevant to the issues raised in the consultation document:

- Under paragraph 7(3)(c) an organization may disclose information without consent when it is required to comply with a subpoena, a warrant or a court order;
- Under paragraph 7(3)(c.1), an organization may disclose personal information to a government institution, including a law enforcement agency,

for the purpose of enforcing a law, carrying out an investigation, gathering intelligence for the purpose of enforcing a law, or administering a law; and

- Paragraph 7(3)(e) allows disclosures without consent to a person who needs the information because of an emergency that threatens the life, health or security of the an individual.

Paragraph 7(3)(c) deals with mandatory disclosures pursuant to a legal authorization.

Paragraph 7(3)(c.1), in contrast, is clearly intended to allow organizations to disclose personal information without consent or notification to LE/NS agencies and other government bodies in the absence of prior judicial authorization. However, the organization requesting the information has to identify its legal authority and indicate that it is collecting the information for one of the reasons listed in the paragraph, for example to enforce a law of Canada, a province or a foreign jurisdiction.

When the legislation (Bill C-6) was being debated in the House of Commons, the Minister of Industry clearly stated that 7(3)(c.1) was intended to maintain the *status quo*, "These amendments do not grant new powers to government institutions, nor do they create new obligations on business." Although 7(3)(c.1) was not intended to alter the *status quo* we appreciate that it may have created some uncertainty on the part of organizations being asked to disclose certain information.

This provision was the subject of a considerable amount of discussion during the mandatory five year review of *PIPEDA* conducted by the House of Commons Standing Committee on Access to Information Privacy and Ethics. In its report, tabled on May 2, 2007, the Committee recommended that consideration be given to clarifying what is meant by 'lawful authority' in section 7(3)(c.1). The Committee also recommended changing the "may" in the opening paragraph of subsection 7(3) to "shall" which seemingly would have made all the disclosures in 7(3) mandatory.

In its response to the Committee's report, table on October 17, 2007, the government indicated that there is a need to clarify the concept of lawful authority. The government rejected the Committee' recommendation about changing "may" to "shall."

The government's response also sought to clarify the overall intent of the paragraph:

> The government wishes to confirm 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*.

The government also indicated that it will examine the possibility of adding a regulation to further define the term "government institution" that is found in 7(3)(c.1) and 7 (3)(d).

Although neither the Committee's report nor the government's response directly referred to 7(3)(e), the government's response stated that it would consider certain limited exceptions to *PIPEDA*'s consent requirements to address the concerns expressed by stakeholders regarding the disclosure of personal information in cases of natural disasters, elder abuse and other similar circumstances. Such a change would undoubtedly be relevant to the issue of disclosing CNA information to LE/NS agencies for emergency purposes.

As the consultation document suggests, at least some of the difficulties that LE/NS agencies face in terms of obtaining CNA information is one of inconsistency. The changes that the government is proposing to make to *PIPEDA* as a result of the five year review may go a long way towards clarifying when and how TSPs may disclose CNA information under 7(3)(c.1) and possibly 7(3)(e).

The Privacy Commissioner has stated publicly that she would not object to adding definition for the terms "lawful authority" and "government institution" if the government feels that such definitions would bring clarity to the legislation.

Although the consultation paper identifies the "absence of explicit legislation" as one of the problems the consultation process seeks to address, *PIPEDA* is, in fact, an explicit legislative code that permits lawful access by LE/NS agencies while "preserving and protecting the privacy and other rights and freedoms of all people in Canada." Before considering legislation that would make the disclosure of CNA mandatory on request, we would strongly recommend that the government determine if the clarification to *PIPEDA* discussed above, together with any guidance that may be appropriate, address the inconsistency. In terms of guidance, Service Alberta has produced a guidance document, "Requesting Personal Information from the Private Sector: Forms and Guidelines for Law Enforcement Agencies", that includes two forms that law enforcement agencies can use when requesting personal information from organizations.[2]

CNA and the Expectation of Privacy

The Consultation document does not define CNA information, but it states that it could include "the following basic identifiers associated with a particular subscriber":

- name;
- address(es);
- ten-digit telephone numbers (wireline and wireless);
- Cell phone identifiers, e.g., one or more of several unique identifiers associated with a subscriber to a particular telecommunications service (mobile identification number or MIN; electronic serial number or ESN; international mobile equipment or IMEI number; international mobile subscriber identity or IMSI number; subscriber identity module card number of SIM Card Number);
- e-mail address(es);

[2] See http://www.pipa.gov.ab.ca/resources/pdf/forms_and_guidelines_for_law_agencies.pdf

- IP address; and/or,
- Local Service Provider Identifier (LSPID), i.e., identification of the TSP that owns the telephone number or IP address used by a specific customer.

Referring to all of this information as customer name and address information is misleading, as is calling these data elements "basic identifiers." This list goes well beyond the customer names and addresses associated with a given telephone number. Some of this information is available through white page directories and reverse directories. However, much of this information is not publicly available; furthermore, much of this information would be unknown to the individuals involved. For example, many people with Internet service do not know their IP address. Similarly, many cell phone subscribers would not even know that there are any identifiers associated with their telephone other than the number.

The assumption behind the consultation paper is that CNA information carries a low expectation of privacy and as such does not require judicial authorization. We disagree: many individuals consider much of this information to be private. First of all, a significant number of people choose to pay extra for unlisted telephone numbers, demonstrating that they consider these numbers to be private. Many people only share their cell phone numbers with friends and family numbers. One of the attractions of the Internet is that it provides an expectation of privacy. Many people use pseudonyms on the Internet in order to engage in anonymous communications and for a variety of other reasons.[3]

In *BMG et al v. John Doe et al* Justice von Finckenstein concluded that it would irresponsible for the Court to order disclosure of the name of an account holder given the uncertainty that exists about the link between the identity of an account holder and an anonymous user as well as the link between the user of an account and a given dynamic IP address.[4]

While some of the this information might be considered less sensitive we need to recognize that it is typically not being sought as an end in itself. CNA information may be valuable to LE/NS agencies specifically because it can provide access to even more sensitive information.

---

[3] See Wilkins J. in *Irwin Toy Ltd. v. Doe* (2000), 12 C.P.C. (5th) 103 (Ont. Sup. Ct.) at paragraphs 10-11: "Implicit in the passage of information through the internet by utilization of an alias or pseudonym is the mutual understanding that, to some degree, the identity of the source will be concealed. Some internet service providers inform the users of their services that they will safeguard their privacy and/or conceal their identity and, apparently, they even go so far as to have their privacy policies reviewed and audited for compliance. Generally speaking, it is understood that a person's internet protocol address will not be disclosed. Apparently, some internet service providers require their customers to agree that they will not transmit messages that are defamatory or libellous in exchange for the internet service to take reasonable measures to protect the privacy of the originator of the information."

[4] *BMG Canada Inc. v. John Doe* [2004] 3 F.C.R. 241.

Section 8 of the Charter of Rights and Freedoms protects Canadian against unreasonable search and seizure when there is a reasonable expectation of privacy. The Supreme Court has recognized that an individual's expectation of privacy may depend on location, the nature of the information and the relationship of the information to the individual. On the third point, one criterion the Court uses in deciding if an individual has a reasonable expectation of privacy is whether the personal information involves "a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state".[5]

In *R v. Plant*, where this concept of "a biographical core of personal information " was first used, the Court found that electricity consumption records did not meet this biographical core test. One consideration used by the Court in reaching this conclusion was that this information is generally accessible by the public. This is not the case with unlisted numbers and cell phone numbers which are fiercely protected by many people indicating a strong expectation of privacy.

In a strong dissenting judgment in *R. v. Plant*, Justice McLachlin (as she then was) noted that

> [c]omputers may and should be private places, where the information they contain is subject to legal protection arising from a reasonable expectation of privacy. Computers may contain a wealth of personal information. Depending on its character, that information may be as private as any found in a dwelling house or hotel room.[6]

Many, if not all, of the various types of personal information included within the ill-named category of "customer name and address" information constitute personal information to which a reasonable expectation of privacy attaches. We strongly recommend that due consideration be given to the *Charter* implications of any legislation that would make it mandatory for a TSP to disclose this personal information when confronted with a warrantless request that is, in reality, a demand.

Proposed Safeguards

The paper proposes a number of safeguards that could be implemented if the government decided to require TSPs to disclose CNA information on request. However, these safeguards only become relevant if one accepts that mandatory disclosure is an appropriate and necessary solution.

We do not propose to comment on the proposed safeguards in any detail. We will comment more fully on possible "checks and balances: and oversight models if legislation is introduced implementing these proposals.

---

[5] *R. v. Plant*, [1993] 3 S.C.R. 281.
[6] *Ibid.*, para. 45.

The consultation paper suggests that agency heads be required to conduct regular internal audits to ensure that any requests for CNA information are being made in accordance with the protocols and safeguards in place. The paper goes on to suggest that audit results be submitted to the Privacy Commissioner of Canada, the Security Intelligence Review Committee, or provincial privacy commissioners, as appropriate.

The paper also refers to explicit provisions to allow the Privacy Commissioner and the Security Intelligence Review Committee to conduct audits related to the release of CNA information.

While after the fact audits are an important means of assessing compliance, they are not a substitute for prior authorization. With respect to our ability to conduct audits with respect to the disclosure of CNA information, our Office can conduct a compliance review of a government department or agency at any time at the discretion of the Commissioner under section 37 of the *Privacy Act*,. Under section 18 of *PIPEDA* we require "reasonable grounds to believe" that an organization is contravening the Act before we can conduct an audit. Although some provincial commissioners may have the authority to audit a provincial or municipal police force in terms of compliance with provincial privacy legislation they do not all have this authority, or the resources to conduct such a review. It is not apparent how the federal government could require a provincial or municipal police force to maintain audit records. This would potentially leave a significant gap in terms of oversight.

Conclusion

The consultation paper is based on a number of assumptions:

1. LE/NS agencies are experiencing difficulties in obtaining access to CNA information that are sufficiently serious to justify new privacy intrusive measures;
2. there is no reasonable expectation of privacy in CNA data;
3. requiring TSPs to disclose this information on request is necessary to address these difficulties; and
4. this approach preserves and protects "the privacy and other rights and freedoms of all people in Canada", as the consultation paper suggests.

We are not convinced that these assumptions are sound. First of all, we do not have a clear sense of the seriousness of the problem. Neither this consultation paper nor previous consultation documents has presented a compelling case based, on empirical evidence, that the inability to obtain CNA in a timely way has created serious problems for LE/NS agencies in Canada. This calls into question the policy rationale from both a proportionality and necessity perspective. Second, it is our view that a reasonable expectation of privacy attaches to CNA data. This renders any mandatory disclosure/seizure regime of dubious constitutional validity.

Assuming there is a well documented and empirically demonstrated problem in obtaining access to CNA information, we are not convinced that requiring TSPs to

disclose this information without a warrant is the only solution or the most appropriate solution. As discussed above, clarifying *PIPEDA* and providing guidance, may go a long way towards resolving this matter. We would also point out that the Canadian Radio-television and Telecommunications Commission (CRTC) has already addressed the issue of access to provider information (LSPID) by law enforcement agencies in Telecom Decision CRTC 2002-21[7]. In that decision the CRTC determined in order to obtain LSPID, a law enforcement agency had to identify its lawful authority to obtain the information and indicate that

1. it has reasonable grounds to suspect that the information relates to national security, the defence of Canada or the conduct of international affairs;
2. the disclosure is requested for the purpose of administering or 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 or administering any such law; or
3. it needs the information because of an emergency that threatens the life, health or security of an individual, or the law enforcement agency otherwise needs the information to fulfill its obligations to ensure the safety and security of individuals and property.

The CRTC's decision uses language similar to that found in subsection 7(3) of *PIPEDA* with the significant addition of the reference to "reasonable grounds to suspect". The CRTC's approach should also be considered.

Finally, we agree with the consultation paper that "the principles and powers of lawful access must be exercised in a manner consistent with the rights and freedoms guaranteed in the *Canadian Charter of Rights and Freedoms*." However, we are not convinced that allowing LE/NS agencies to obtain CNA information on demand would meet this threshold. As discussed above, we do not accept the premise that individuals have a low expectation of privacy with respect to the information in question and that obtaining this information without judicial authorization would protect "the privacy and other rights and freedoms of all people in Canada."

---

[7] Telecom Decision CRTC 2002-21, 12 April 2002, Provision of subscribers' telecommunications service provider identification to law enforcement agencies.

Ian Kerr
Canada Research Chair in Ethics, Law and Technology
Principal Investigator

ON tHE IDENTITY TRAIL

Customer Name and Address Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON, Canada K1A 0P8

October 19, 2007

Dear Sir/Madam,

Re: CUSTOMER NAME AND ADDRESS CONSULTATION

1. In response to your invitation for comments on "updating Canada's lawful access provisions as they relate to law enforcement and national security officials' need to gain access to CNA [Customer Name and Address] information in the course of their duties",[1] please accept these comments and the attached article as our submission.

2. The government's Consultation Document on CNA proposes a number of law reform initiatives similar to those embodied in the 2005 Bill C-74, *The Modernization of Investigative Techniques Act*.[2] It was in light of Bill C-74 that the attached article, entitled *The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers*, was written.[3] In the article, we describe the changing role of telecommunications service providers (TSPs) from trusted gatekeepers of clients' privacy to active partners in the fight against cybercrime. We argue that the legislative approach proposed in Bill C-74 will lower the threshold of privacy protection and significantly alter the relationship between TSPs and the individuals who have come to depend on them to manage their personal information and private communications. We believe this article is pertinent to the current consultations on CNA information, and have attached it here for your consideration.

3. We must begin by expressing concern about the course that the current round of consultations on access to CNA has taken. The closed-door consultation initially commenced by Public Safety Canada, along with Industry Canada, excluded many interested stakeholders that the government needs to hear from if the consultation process

---

[1] "Customer Name and Address Information Consultation", online: Public Safety Canada http://securitepublique.gc.ca/pgs/ns-cnaci-eng.asp [Consultation Document].

[2] Bill C-74 died with the dissolution of the Liberal government. An identical bill was later introduced by Liberal M.P. Marlene Jennings as a private member's bill (Bill C-416), but this bill also died on the order paper when Parliament was prorogued.

[3] This piece was published in (2007) *Criminal Law Quarterly*, vol. 51(4) 469.

Faculty of Law
Common Law Section
57 Louis Pasteur
Ottawa, ON K1N 6N5 Canada
Tel.: (613) 562-5800 ext. 3281 • Fax/Télec.: (613) 562-5417
ankerr@uottawa.ca

Faculté de droit
Section de common law
57, rue Louis-Pasteur
Ottawa, ON K1N 6N5 Canada

is to be participatory and truly representative of public interests. We are hopeful that in future consultations Public Safety Canada will ensure that the discussion is open and accessible from the outset, and not made public merely as the result of political necessity.

The Goal : Balancing Interests

4. The Consultation Document broadly identifies the objective of the proposed lawful access regime regarding CNA information as "...to maintain lawful access for law enforcement and national security agencies in the face of new technologies while preserving and protecting the privacy and other rights and freedoms of all people in Canada," and ensuring "that the solutions adopted do not place an unreasonable burden on the Canadian public."[4] The proposed solution provides for legislation under which law enforcement and national security officials could access CNA information from TSPs without a warrant, court order or other judicial authorization, and without reasonable grounds to suspect criminal activity.

5. It is our submission that while the Consultation Document correctly recognizes the need to carefully weigh the interests of law enforcement and national security with individual civil liberties, the access to CNA scheme under consideration does not strike an appropriate balance. Legislating 'on-demand' access to CNA information without judicial authorization poses serious risks to the privacy interests of Canadians.

6. In light of our concerns regarding the privacy implications of the proposed scheme on lawful access to CNA information, we are pleased to support the recent statements of Public Safety Minister Stockwell Day on September 13, 2007, confirming that the government will not introduce legislation compelling the disclosure of CNA information without a court order:

> We have not and we will not be proposing legislation to grant police the power to get information from Internet companies without a warrant. That's never been a proposal. It may make some investigations more difficult, but our expectation is rights to our privacy are such that we do not plan, nor will we have in place, something that would allow the police to get that information.[5]

7. We agree with Minister Day for the following reasons.

CNA Information

8. The Consultation Document indicates that the CNA information collected by law enforcement could include a range of basic identifiers associated with a particular TSP subscriber, including: name, address(es), telephone numbers (wireline and wireless), cell

---

[4] Consultation Document, *supra* note 1.

[5] Cathy Weeks, "Warrant needed to pull data on Internet users: Day" *The Ottawa Citizen* (14 September 2007), online: The Ottawa Citizen http://www.canada.com/ottawacitizen/news/story.html?id=af578ca9-[illegible]-4785-9939-58364e4158a3.

phone identifiers, email address(es), IP address(es) and/or local service provider identifier information.

9. The proposal for warrantless access to CNA information is based on the mistaken premise that this information is the least revealing form of personal data, in which individuals have the lowest expectation of privacy. This assumption does not hold true, particularly in the context of electronic communications. CNA information, like name and address, are keys to acquiring other personal information, including highly sensitive data such as health or financial records.[6]

10. Intensifying our concerns about unfettered access to CNA information are the realities of data mining. Information collected and stored for one purpose can be combined with information collected and stored for a completely different purpose through data mining, and two pieces of seemingly innocuous information can prove damning in combination. While CNA data may appear less revealing, and is therefore deemed less worthy of strong privacy protections, in combination it can be just as, or even *more* revealing as other kinds of sensitive data in which individuals may have a greater expectation of privacy.

11. The creation of expedited, warrantless procedures for accessing CNA information is based on the false assumption that CNA data is somehow a lesser form of investigatory information. The possibility of legislating unrestricted access to this kind of information poses a serious threat to the individual privacy of Canadians. By erecting false distinctions between different kinds of data, and treating these categories of information differently, the government is in fact seeking enhanced search powers through expedited processes and lower standards, thereby slashing privacy safeguards and expectations.

12. The Consultation Document assures that the scope of CNA information subject to 'on-demand' disclosure "...would not, in any formulation, include the content of communications or the Web sites an individual visited while online."[7] The potentially revealing nature of CNA information when in combination with other data make it impossible to guarantee that online activities and communications will not be captured, inadvertently or otherwise, within the proposed scheme. The point cannot be sufficiently underscored: *typical subscriber information of the sort made available under the proposed legislative scheme will become the means by which a biographical core of personal information is assembled.*

Proposed Safeguards

13. Empowering law enforcement officials to obtain CNA information in an expeditious manner simply by asking for it represents a significant alteration in the procedural safeguards against excessive 'fishing' expeditions by law enforcement agencies. Under

---

[6] The Ontario Court of Justice recently acknowledged this reality, stating, "[i]nformation about name and date of birth is information which can be a key in unlocking other database information about an individual of an intimately personal nature." See *R. v. M.E.*, [2006] ONCJ 146 at 32.

[7] Consultation Document, *supra* note 1.

the existing system, the primary safeguard against police abuse of investigative powers is the requirement for judicial pre-authorization, based on a "reasonable grounds" standard to suspect criminal activity, before police can conduct a search or surveillance activity. The proposed access scheme will eliminate this safeguard in respect of CNA information. For this reason, we cannot support the proposal.

14. Allowing law enforcement officials to obtain unlimited amounts of CNA information simply by asking for it, with no accountability apparatus in place represents an infringement of the privacy rights and expectations of Canadians. Law enforcement should be made to justify requests for access to information at a high standard before judicial authorization is granted. These orders should not be available for suspicions or anticipated crimes, for example, but only when authorities believe that an offence has been committed. Law enforcement should be required to demonstrate that there are reasonable grounds for requesting data, and the scope of authorization should be construed as narrowly as possible, on a standard of necessity, not relevance to the investigation.

15. We have considered the 'alternative' safeguards proposed in the Consultation Document, including:

- requiring the designated officials to record their status as such when making a request, as well as the duty or function for which a particular request is make;
- limiting the use of any information obtained to the agency that obtained it for the purpose for which the information was obtained, or for a use consistent with the purpose, unless permission is granted by the individual to whom it relates; and
- requiring regular internal audits by agency head to ensure that any requests for CNA information are being made in accordance with the protocols and safeguards in place.[5]

16. We are unable to conclude that these safeguards go far enough in protecting privacy interests when weighed against the fact that police would have 'on-demand' access to CNA information under the proposed scheme. Permitting warrantless access to CNA information "...for the purpose of performing an official duty or function"[6] remains, in our submission, an overbroad proposal. Without judicial oversight, the purposes for which law enforcement may demand CNA information must be narrowly and precisely circumscribed.

Constitutionality

17. The Consultation Document explicitly states, "[t]he principles and powers of lawful access must be exercised in a manner consistent with the rights and freedoms guaranteed in the *Canadian Charter of Rights and Freedoms*..."[7] We could not agree more, and it is with *Charter* principles in mind that we ask you to consider the constitutionality of

---

[5] Consultation Document, *supra* note 1.
[6] *Ibid.*
[7] *Ibid.*

allowing warrantless access to CNA and related information. In our view, the proposed access proposal would not survive *Charter* scrutiny in a Canadian court of law.

18. Section 8 of the *Charter* protects Canadians against unreasonable search and seizure,[11] and the Supreme Court of Canada has equated this guarantee with the existence of a reasonable expectation of privacy.[12] The information within which one has a reasonable expectation of privacy has been found to include a "biographical core of information",[13] or information that tends to reveal intimate details about the individual. Legislation authorizing unwarranted access to CNA information could be challenged under section 8 on the grounds that it amounts to an unreasonable search and seizure because the potentially revealing nature of CNA information invades the "biographical core" of information within which individuals have an expectation of privacy. As stated above, CNA information can be linked with online activities and communications as well as other sensitive documentation that may reveal intimate details of an individual's life.

19. Only if a *Charter* breach cannot be "demonstrably justified in a free and democratic society"[14] will the law be declared unconstitutional. This analysis takes place under section 1 of the *Charter* in accordance with the test set out by the Supreme Court of Canada in *R. v. Oakes*.[15] In assessing the proposed lawful access regime for CNA information, the appropriate constitutional question under section 1 is whether the pressing and substantial objectives of the legislation are proportional in terms of being a) rationally connected to the objective; b) minimally impairing of rights; and c) proportional to its potentially harmful effects. We say that they are not.

    a. The relevant question with respect to the rational connection between the proposed means and the objective of warrantless access legislation is whether the breadth of expansion in investigatory powers, the reduction of procedural safeguards, and the expedited means by which law enforcement agencies could access personal information about citizens without oversight, as set out in the Consultation Document, is proportional to the objectives it seeks to fulfill. In our view, the current proposal is an excessive and over-inclusive response. Canadian law enforcement and national security have demonstrated an ability to investigate and prosecute cybercrime and has even garnered international success in online investigations,[16] and has done so without warrantless access to CNA information.

---

[11] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the Canada Act 1982 (U.K.), 1982, c.11, s.8 [*Charter*].

[12] See e.g. *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145.

[13] *R. v. Plant* [1993] 3 S.C.R. 281 at 293 [*Plant*].

[14] *R. v. Oakes*, [1986] 1 S.C.R. 103 at 69-71.

[15] *Ibid.*

[16] See e.g. "Toronto police find hotel where child-porn pictures taken" *CBC News* (4 February 2005), online: CBC Online <http://www.cbc.ca>; "Toronto Police use internet to save sexually exploited girls" *CBC News* (26 March 2004), online: CBC Online <http://www.cbc.ca>; "Web expands to fight online sex crimes" *Edmonton Journal* (5 June 2005) A6; "Online trail can lead to Court" *The New York Times* (4 February 2006) 1.

b. 'On-demand' access to CNA information invites law enforcement officials to an all-you-can-eat 'investigatory smorgasbord' with no say on the part of the citizens concerned about the collection, use, or disclosure of their personal information. In absence of judicial pre-authorization, the safeguards proposed in the Consultation Document provide only minimal restrictions on who can access subscriber information and under what circumstances, and offer no real oversight mechanism to monitor the process. The excessive range of personal information available, in conjunction with the lack of accountability measures in place to monitor expedited access does not impair *Charter* rights as minimally as possible.

c. Without sufficient safeguards, it is impossible to ensure that legislation imparting unfettered access to subscriber information will not be misused by law enforcement for excessive information gathering or for other purposes unrelated to cybercrime activity. The potential for disproportionately deleterious effects is therefore unreasonably high. In light of the ease with which CNA information can be combined to reveal intimate aspects of one's life, it is not difficult to imagine the damaging consequences that could result if one's health, financial or other personal information was improperly collected, used or disclosed. In fact, the courts have recognized this possibility and noted that it "is capable of creating substantial hardship."[17]

20. It is our submission that unwarranted access to CNA information amounts to an unreasonable search and seizure, and that legislation permitting such searches in the absence of sufficient oversight mechanisms would violate the *Charter*. A society which lays bare our personal information with insufficient democratic safeguards may be perfectly suited to fight cybercrime, but, as the Supreme Court of Canada has noted, also "has the potential, if left unregulated, to annihilate any expectation that our communications will remain private."[18]

Conclusion

21. While the proposed legislation may make it easier and more convenient for law enforcement officials to undertake cybercrime investigations, ease and convenience are not sufficient justifications for violating the privacy rights of Canadian citizens. The possibility of opening up CNA information to law enforcement official is an excessive and over-inclusive response by the government that undermines citizens' fundamental privacy rights in a manner that cannot be justified in a free and democratic society.

Sincerely,

Ian R. Kerr Jena McGill Daphne Gilbert

---

[17] *Plant, supra* note 13.
[18] *R. v. Duarte*, [1990] 1 S.C.R. 30 at 22.

Canadian Association of Chiefs of Police ***Leading Progressive change in policing***
Association canadienne des chefs de police ***À l'avant-garde du progrès policier***

October 24, 2007

The Honourable Stockwell Day, P.C., M.P.
Minister of Public Safety
Sir Wilfrid Laurier Building
340 Laurier Avenue West
Ottawa, Ontario
K1A 0P8

Re: Customer Name and Address
Consultation

I write in response to your call for submissions concerning timely access for police to customer name and address information or what is commonly referred to as "CNA."

Through our Law Amendments Committee and the Lawfully Authorized Electronic Surveillance (LAES), the CACP has consulted extensively with your officials and the need to maintain our lawful access capabilities. As part of this process, we have provided many examples where timely access to CNA is vital to public safety and the investigation of crime. The CACP supported the CNA legislative regime contained in Bill C-74, the Modernization of Investigative Techniques Act. We believe it struck the appropriate balance between the legitimate needs of the public safety and the privacy concerns of Canadians. I therefore urge you to consider including the CNA provisions in your governments Lawful Access Bill.

Our committee will continue to make themselves available to your officials to ensure this vitally important legislature is enacted with all due haste.

Yours truly,

Steven Chabot

Deputy Director General Steven Chabot
President, CACP

582 Somerset Street West/582, rue Somerset, Ouest Ottawa, Ontario K1R 5K2
Tel: (613) 233-1106 • Fax/Télécopieur: (613) 233-6960 • E-mail/Courriel: cacp@cacp.ca

David H. Hill, C.M./Q.C., Lynda A. Bordeleau General Counsel/Conseillers juridiques
Perley-Robertson, Hill and McDougall LLP Barristers & Solicitors/Avocats et Procureurs

CUSTOMER NAME AND ADDRESS (CNA) INFORMATION CONSULTATION

NCECC – RCMP SUBMISSION TO PUBLIC SAFETY CANADA

October 2007

INTRODUCTORY REMARKS

The National Child Exploitation Coordination Centre (NCECC) of the Royal Canadian Mounted Police (RCMP) welcomes the opportunity for broader public consultation on "issues associated with the question of accessing customer name and address in the modern telecommunications world."[1] NCECC would like to state at the outset that a legislative solution is becoming essential. It is needed to require or compel telecommunications companies to provide basic customer identifying information to police upon receiving a formal request. Without a statutory requirement imposed on them, these companies can choose (under the common law) to do nothing. Even though police have a longstanding authority under the common law to ask people questions in the lawful execution of their duties, there is nothing presently in legislation to require these companies to respond positively.[2] As long as they 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 actually cannot proceed. Misunderstandings surrounding the common law authority of police to seek this information without having to first obtain a court order have already had serious consequences for child exploitation investigations and victims.

Since the establishment of NCECC in 2004, 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) . However, it is important to note that NCECC operations are not the only operations that are seriously affected. The "CNA problem," as police tend to call it, has been on law enforcement's radar screen, becoming an increasing impediment to effective police operations, since early 2000.[3]

---

[1] "Customer Name and Address Information Consultation" document posted at http://publicsafety.gc.ca.

[2] See *R.* v. *Turcotte*, [2005] 2 S.C.R. 519 at para 41 where the Supreme Court of Canada (SCC) noted: "Under the traditional common law rules, absent statutory compulsion, everyone has the right to be silent in the face of police questioning.

[3] Canadian Association of Chiefs of Police, "Response to Government of Canada's Lawful Access Consultation Document", 16 December 2002, http://www.cacp.ca. The CACP, in 2002, noted at p. 1-2:

> [W]hile communications technology has continued to rapidly advance, the ability of police to retain access capabilities and gather the necessary information to detect and apprehend criminals has not. This gap in the relationship between law and the reality of today's technology now poses a significant threat to public safety and the attenuation of police effectiveness. It is creating a safe zone where serious criminals, such as organized crime and cyber predators, can operate free from fear of detection and apprehension. … Internet Service Providers have been very reluctant to

The NCECC finds that the Internet has created an environment where sexual offenders can operate with increased anonymity, while police operate with increased difficulty accessing their basic identifying information. The NCECC attributes this growing phenomenon to the misconception that a customer's name and address, when the customer is online, is more private and should have more protection from reasonable police access than the name and address of a telephone customer that appears in a telephone book.

In this submission, the NCECC will be discussing the CNA issue mainly in the context of investigating Internet facilitated child exploitation. However, the impediments that NCECC investigators as well as other police officers encounter routinely in trying to identify offenders on the Internet, are not unique to investigative operations. Police face challenges obtaining CNA in all their mandated work, that is, from general (non-investigative) policing duties to investigations of the most serious criminal offences. Consequently, many of the observations that the NCECC will be making in this submission apply to all aspects of RCMP operations, and indeed to the work of all police agencies in Canada.

Police understand, value, and respect the importance of protecting individual privacy. We also understand that privacy interests must be balanced with other public interests, for example, the public interest in keeping members of our communities safe, in preventing injuries and crime, and in successfully charging criminals for their offences. In our experience the success of policing operations in our communities depends on ensuring that a reasonable balancing of these interests is achieved.

The NCECC understands that the legislative proposals, which have been under consideration for the past few years, were designed to create an administrative framework to govern requests for customer information. That framework would include clear legal rules both for police to obtain and for telecommunications companies to release basic customer identifying information, such as a customer's name and address.

Much of the public debate surrounding police access to customer name and address information, so far, has concentrated only on one issue – whether police should, or should not, be required to obtain the prior authorization of a court in order to lawfully access this information. The NCECC will address that important question in this submission. In addition, this submission will attempt to explain why the RCMP, including the NCECC, has reached the conclusion that legislative support is necessary, and why in the RCMP's view the proposed administrative model --rather than criminal legislation creating a new warrant or court order -- is the logical choice for police to obtain this information.

The remainder of this submission consists of two parts. The first part outlines the challenges and issues that arise for the NCECC (and the RCMP generally) in seeking to identify users of Internet services. The second part discusses law enforcement's

---

provide information about registered users even when these clients are engaged in dangerous criminal behaviour.

preferred solution: legislation adopting an administrative model to govern how police and telecommunications companies handle requests for information identifying their customers.

PART ONE:
CHALLENGES & ISSUES FROM A POLICING PERSPECTIVE

The Internet has revolutionized our lives in a tremendously positive way but it also poses significant risks to adults and children. For adults the risks are mostly economic; however, for children the risks are to their personal safety and security.

Historically, Canadian law has been predicated on the belief that community safety was a mutual goal and for that reason, until very recent times, there have been few laws needed to compel the cooperation of certain sectors. Unfortunately, in the online world, the sense of a civic duty or public responsibility to assist police, for example with identifying customers, appears to be diminished. The state can no longer count on the voluntary cooperation of certain corporate citizens in the online world to ensure community safety.

In the past telephone companies were the traditional source of customer name and address information for police. They voluntarily assisted by providing basic name and address information to identify customers using their services. Today certain companies as well as Internet Service Providers (ISPs) resist and regularly refuse to assist in this way. For these companies this change may be due in part to legal obligations they have had since 2000 to protect the privacy of their customers' personal information, confusion over the "lawful authority" of police to request this type of non-sensitive customer information without first obtaining a warrant, and their desire to avoid potential litigation and corporate liability for alleged privacy violations. As a result, police now find themselves asking federal lawmakers to contemplate enacting laws compelling these companies to provide this basic customer identifying information to police.

The NCECC notes that some critics have opposed these proposals because they consider such new laws to be an unjustified extension or increase in police powers. However, it is the view of the RCMP, including the NCECC, that these proposals would not provide police with "new" powers. Rather they would be legislative provisions confirming an established authority police have under the common law. The proposed legislation, in effect, would compel telecommunications companies to cooperate in situations where certain companies now exercise their right under the common law to say nothing. As a result, the legislation would affirm the existing authority of police to ask, while clarifying for companies that they must provide this particular information on request.

Federal lawmakers have been asked by the CACP and other policing organizations to resolve the "CNA problem" in order to preserve the ability of police to continue to obtain non-sensitive customer information upon request (and without a warrant). From an operational perspective, this proposed legislation would enable police to regain lost

ground in terms of being able to readily acquire non-sensitive customer information that is critical to the effectiveness of daily police operations.

In the remainder of this Part, the NCECC will be discussing the following considerations, which we believe to be important in assessing how to resolve the challenges that police are facing in obtaining CNA and other basic customer identifying information:

1. Problems with the status quo;
2. Police are not requesting personal information that is confidential or sensitive;
3. Warrants may not be feasible or possible to obtain this basic information;
4. Unnecessary demands for warrants place an added burden on the Justice system;
5. Time delays, resource impacts, consequences for victims;
6. Public expectations of police;
7. ISP obligations;
8. Statistics supporting the need for legislative response; and
9. Public support for police efforts.

1. Problems with the status quo

The NCECC would like to note that the level of cooperation by Canadian ISPs ranges from excellent to non-existent. Many of the large Canadian ISPs in this country are willing to assist and usually meet, and occasionally exceed, our expectations when called upon for assistance. Our success in rescuing children and investigating offenders who pose a risk to children, is a direct result of their cooperation. However this is not universal amongst all ISPs. Our statistics of thwarted investigations at the NCECC averages 33%. One third of all requests, per month are refused, not responded to, or we are advised that the data is no longer available. A few small ISPs openly advertise their lack of cooperation with police to attract customers.

The cooperation NCECC does enjoy is the result of more than two years of negotiation and legal analysis by ISPs' legal counsel who form part of the Canadian Coalition Against Internet Child Exploitation (CCAICE). This coalition is comprised of ISPs, government representatives, Cybertip and interest groups. Together we have developed an administrative process very similar to proposals made to address the CNA issue with an administrative framework set out in legislation. The difference is that the CCAICE model is voluntary and ISPs are not required by legislation to do anything to assist police. As a result, numerous impediments and many outstanding issues arise with the CCAICE model. They include:

I. **Inconsistent Cooperation:** Since participation of ISPs is completely voluntary, they may withdraw at any time. There are apparently over 400 Canadian ISPs. Many are not participating fully and consistently.

II. **Refusal to Cooperate**: Some ISPs constantly refuse to cooperate. Currently five ISPs are known to do so. Furthermore, after police approach them for assistance to identify the individual associated with an IP or email address, there is nothing prohibiting the ISP from informing their customer about the police inquiry.

III. **Delays:** There are no obligatory time frames for assisting police. For example, in one case while investigating real-time on-line sexual assaults the investigator requested CNA in an effort to locate and rescue the children. The ISP advised the investigator to call back after the weekend and during business hours.

IV. **Unenforced Customer Agreements:** ISP customer agreements indicate that ISPs will cooperate with police if the customer is using the service to break the law. However, these agreements are between the service provider and their customers. They do not create any legal obligation for ISPs to assist police by helping to identify persons committing offences online. That type of assistance is voluntary.

V. **Unreported Criminal Behaviour:** Although most ISP customer agreements prohibit unlawful activities and stipulate that they will report criminal acts, NCECC was able to locate only one instance where a Canadian ISP had discovered suspected child pornography and reported it to the RCMP.

VI. **Investigative Limitations:** Participating ISPs will only voluntarily provide CNA in Internet facilitated child sexual abuse cases. Requests for CNA related to other criminal investigations and public safety threats are normally refused. So, if police are alerted to a person who has posted threatening material on the Internet and who may pose a serious risk to public safety, currently they cannot count on the assistance of that person's ISP to identify him. In the aftermath of a recent school shooting, it was discovered that the shooter had posted disturbing material on the Internet. This incident highlights potential dangers that might be averted if police were actually able to obtain CNA when public safety could be at risk.[4]

VII. [redacted]

VIII. **Inaccurate Information:** Some ISP's stipulate that they cannot or will not ensure the accuracy of the CNA information provided.

---

[4] See e.g,, http://www.cyberpresse.ca/article/20060914/CPACTUALITES/60914017/6096/CPACTUALITES. Here it was reported:

> On peut également voir dans des quotidiens des photos du suspect sur un site web. Kimveer Gill y exhibe fièrement plusieurs armes. Il y a pratiquement laissé sa biographie dans laquelle le jeune homme se décrivait comme un solitaire qui ne s'entendait pas avec ses parents, qu'il était très tourmenté et détestait les sportifs et la société en général. Il a notamment écrit qu'il souhaitait mourir soit «comme Roméo et Juliette ou sous une pluie de balles.»

IX. **Email Addresses Versus IP Addresses:** Many ISPs are unwilling to provide the NCECC with CNA from an email address rather than an IP address. NCECC is unable to explain why ISPs make this distinction.

In an effort to gain further cooperation there have been numerous meetings, telephone conferences, consultations with corporate legal counsel, the support and intervention of proactive ISP counsel and counsel from the Ontario Attorney Generals office. However, despite these ongoing efforts, the NCECC has failed to sway some companies.

The CCAICE administrative model was a welcome initiative and in NCECC's view one of the most significant undertakings, to date, by the Canadian Coalition Against Internet Child Exploitation. Nevertheless, in light of these shortcomings, NCECC, the RCMP and other police forces now find themselves asking federal lawmakers to contemplate enacting laws compelling these companies to provide basic customer identifying information to us.

2. <u>Police are not requesting personal information that is confidential or sensitive</u>

Judicial authorizations, such as warrants, are designed to protect people's reasonable expectation of privacy. A judge's order is necessary to protect the sanctity of places where an individual has this expectation (for example, home, office) or information that attracts this expectation (for example, an individual's core biographical information such as DNA, medical records, chat logs, and web-surfing history).

While a warrant is required to obtain an individual's core or sensitive biographical information, warrants are not required to access non-core or non-sensitive biographical information. A person's name, address, and phone number, is personal information that is not sensitive -- it is *not* core biographical information about the person. This information does not reveal intimate details about an individual's lifestyle and personal choices. So when police request this information they are not seeking information that is confidential or core biographical information. This type of information is made widely available through numerous avenues, such as call display, phone books and reverse phone number look-up on the Internet.

The public debate surrounding police access to customer information upon request seems to pit privacy interests against the state's interest in protecting the public and investigating crime. The prevailing premise seems to be that the two interests are mutually exclusive. However, it is the RCMP's view that these interests must co-exist and the best interests of Canadians are met by balancing both interests rather than by one winning out over the other. The Supreme Court of Canada articulated that important balance very well by stating "The community wants privacy but it also insists on protection. Safety, security and the suppression of crime are legitimate countervailing concerns." (*R.* v. *Tessling*, [2004] S.C.J. No. 63 at para. 17).

Furthermore in *Tessling*, the Court pointed out that "not every form of examination conducted by the government will constitute a search for constitutional purposes." In *R.* v. *Plant* the Court also clearly established that not all information an individual may wish to keep confidential necessarily enjoys s. 8 protection. (*R.* v. *Plant*, [1993] S.C.R. 281 at 293).

3. Warrants may not be feasible or possible to obtain this basic information

The BC Court of Appeal recently dealt specifically with the issue whether a police request to obtain the name and address of a customer related to certain bank account numbers, so that police could prepare an ITO (information to obtain a warrant), violated the accused's reasonable expectation of privacy. The Court found: "Section 8 of the *Charter* provides that everyone has the right to be secure against unreasonable search. In the case at bar I am of the opinion that there was no search, much less any unreasonable search as envisioned in the *Charter.*" (*R.* v. *Quinn*, [2006] B.C.J. No. 1170 at para. 93).

A police request for a customer's name and address related to an Internet account indicates only who is financially responsible for the account. Further investigative steps must be taken to determine who accessed the computer and who may be responsible for the crime. A warrant for the residence or computer would be obtained only once police gather sufficient information to form reasonable and probable grounds as to who may be culpable and determine where evidence is likely to be found.

In the case of Internet facilitated child sexual exploitation offences in Canada, the investigation normally begins when a seizure of evidence from one offender reveals Internet Protocol (IP) addresses of other offenders who have uploaded, downloaded, and/or shared child pornography. When computers "speak" to each other, the IP address is automatically captured along with the date and time of communication. Police then commence a new and separate investigation to identify those responsible.

For example, a recent child pornography case from Germany identified 28 countries and within Canada over 200 IP addresses. Upon receipt, the NCECC attempted to identify the account holders. They were unable to identify the account holder information of 47 of the IP addresses due to the lack of ISP cooperation. In this case, and other examples like it, the investigation begins with, and often ends without, police finding out the name and address of an account holder who was using an IP address assigned by a service provider on the day and time in question.

Police must ask the ISP for the customer name and address associated to each IP address – the ISP is the only one who has that information. At the time of the request, police are at the preliminary stages of an investigation, operating on unsubstantiated information (suspicion) in an investigative process that may or may not establish reasonable grounds. This stage of information gathering is sometimes referred to as the "pre-warrant stage" of an investigation. 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.

Police regularly receive complaints from the public regarding postings where, among other things, people harass others, threaten suicide or display aggressive behaviour. These matters require follow-up to determine if there is an offence and/or if someone is in danger or in need of assistance. This is a critical public safety responsibility assigned to police both on and off line. Unfortunately situations, which begin as these types of complaints, can turn into cases such as criminal harassment, hate crimes, and uttering threats over the Internet and some have the potential to result in injury or death.

In the early stages of police handling this type of matter, police need to identify and / or locate the person involved. The first step in that process is to try to obtain from the ISP the necessary information to identify the Internet customer. If the ISP will not assist police with that first step then their first step often becomes their last step. The ISP is the only one who holds the customer information in question. Police would not have sufficient grounds to form the reasonable belief an offence has been committed, which is required to obtain a warrant or court order, so the police's capability to inquire into the matter would cease with the ISP's refusal to cooperate.

Unlike vehicle license plates, there is no central database for the police to query to identify the individual registered to an ISP's system as the source of a particular IP or e-mail address. Only ISPs have this information and, when they are contacted to provide that information, a number of them routinely refuse such requests.

Other industries readily assist police in identifying persons of interest in the early stages of investigations of offences that occur without the involvement of the Internet; however, when the crime involves the Internet police routinely are faced with having to convince an ISP of their lawful authority to request this information. Without a specific provision in the law to point to as their statutory authority to obtain this information upon request, police are faced with quoting Charter jurisprudence to company personnel and explaining their general statutory powers and common law authorities to them.

Several police responsibilities do not involve criminal investigations but instead involve assisting the public. They are referred to as general policing duties and while they form part of police officers' core responsibilities, they do not involve the investigation of crimes or other offences. However, they also can involve police in seeking to identify the names and addresses of certain people.

These duties, for example, include but are not limited to: notification of next of kin; investigation of reports of "overdue" (not yet officially missing) spouses, hunters and hikers; search and rescue for missing persons; assistance to individuals apprehended under mental health legislation; and assistance to a Coroner in the identification of deceased persons.

A report to police by parents of an "overdue" child is a general policing duties scenario that illustrates a situation where an officer may need to turn to an ISP for assistance in identifying a customer's name and address. When the report (phone call from the

parents) is received, the child is not yet confirmed to be missing and police do not have grounds to believe there has been foul play. Therefore, the facts of the case have not ripened into a criminal investigation. The parents could simply report, for example, that their 11 year old daughter did not return home at the pre-arranged time from playing at the park down the street and they suspect she might have gone to meet her online friend: Johnnie4@small_ISP.ca. When they call police for assistance in locating their daughter, an officer would try to follow-up on their "meeting" tip by seeking the assistance of the parent's ISP in identifying the source (customer name and address) of the Johnnie4 email address. The officer would be trying to gather some basic identifying information related to the source to use in figuring out who he might be -- he might just be a friend in their daughter's class or he could be a convicted sex offender. The ISP customer name and address information would not, of course, tell the police whether Johnnie4 is a friend or a dangerous adult. It would simply lead police closer to making that assessment. However, if small_ISP won't voluntarily give police the name and street address associated with the email address of Johnnie4, then the ability of police to follow-up on the parents' initial lead would be thwarted. This scenario does not involve an investigation, at this stage, where a warrant would even be possible. At this point, a child is overdue and may be missing but police do not have any grounds to believe, or even suspect, an offence has been committed. It is however an important police matter where time is of the essence and where the parents', the police's and the public's expectations are high for police to be able to assist in locating the child and to act quickly.

In these cases, where police are either performing general duties (not investigating a crime) or their investigation is at such a preliminary stage that a warrant would be impossible to obtain, police depend on moral suasion and a service provider's sense of civic duty to obtain their cooperation. It is simply not legally possible to obtain a warrant under the *Criminal Code* at this "pre-warrant" stage of a matter. Without an ISP's cooperation, the matter may be closed before it can ripen into a criminal investigation. This type of result is unsatisfactory to police, as well as complainants and the public. In missing children and child exploitation cases, NCECC is concerned that this type of result is particularly unacceptable for the children who are the victims and need to be rescued.

In addition to the situations described above, where obtaining a warrant or court order is **not possible**, sometimes (where it would be possible to obtain the order) it is **not feasible**. In these situations obtaining a court order, such as a production order under s. 487.012 of the *Criminal Code* for an ISP customer's name and address, would be possible because police have reasonable grounds to believe an offence is being committed. However, in these particular cases the customer name and address information, to be useful, is required immediately. An example of this type of situation comes from a recent online fraud investigation.

[redacted]

[redacted]

4. Unnecessary demands for warrants place an added burden on the Justice system

In addition to situations where timing and an immediate need to obtain CNA defeats the purpose of obtaining a warrant, the NCECC and other RCMP investigators have encountered situations where they find service providers are forcing them into obtaining a warrant or order from a court, even though one is not required under the law. In these cases, RCMP needs information to identify a customer but the information in question does not attract a reasonable expectation of privacy and so the prior approval of a court is not required by law. Nevertheless, the service provider -- who is the custodian of the customer information -- refuses to provide it unless police produce a court order or warrant for the information.

For example, law enforcement officers investigating child sexual exploitation offences are often forced into preparing warrants to obtain a customer's "personal information" in circumstances where authorizations are not required by law. They do so to appease liability concerns of certain ISPs who want the clear protection that a warrant can offer

against potential liability if an ISP is later accused of disclosing a customer's personal information contrary to the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[5] Faced with a choice between being able to save a child enduring grievous sexual abuse or unnecessarily using police and court resources to obtain a warrant to satisfy an ISP's concerns, police in some regions have determined that they have no option but to capitulate.

Police in New Brunswick recently completed an extensive investigation and arrested seven suspects on the same day. While the arrests and charges are indicative of the quality of the investigation, it required double the work as uncooperative ISPs demanded warrants before they would produce CNA information for police. Seven search warrants were drafted to compel the ISPs' cooperation rather than because they were required under the law in order to protect a reasonable expectation of privacy. Thus, a total of 14 warrants were obtained in that case, doubling this work for police and the courts.

When compared to other telecommunications service providers, such as the major telephone companies, as well as other industries, certain ISPs are unique among them in terms of the frequency with which they demand warrants for this type of basic customer information before assisting an investigation. Many other companies willingly assist police in similar circumstances to further their work in the prevention, detection, and early stages of investigation of crimes.

It should be noted that other industries, in particular, provide information willingly to police without demanding warrants or questioning the definition of "lawful authority". For example, in a Canadian homicide investigation, the victim's body parts were found in various companies' shopping bags and investigators had already identified an area of the city where the suspect was believed to be residing. So, they contacted these companies and asked for a list of the names and addresses of any customers who lived in this area. If any particular individual then surfaced on several customer lists, he would have been of increased interest to the homicide investigators as a potential suspect. While the killer was ultimately identified via other means, this call for company assistance occurred at a pre-warrant and early stage of investigation. In the end their voluntary cooperation may, or may not, have provided the only clue possible to crack the case. But the point is that these companies did not hesitate when they were asked to volunteer non-sensitive customer information for the purposes of a murder investigation. Their actions demonstrate how good corporate citizenship can facilitate investigations and that other sectors do not demand warrants for non-sensitive customer information.

Historically, telephone companies voluntarily assisted police; however, police now find that these telecommunications service providers, in particular some cellular telephone service providers, are also increasingly reluctant to cooperate.

For example, recently a RCMP police officer had his cell phone stolen. His service provider required him to give written permission to local police so that they could access his telephone records during their investigation. In spite of having the customer's

---

[5] S.C. 2000, c. 5, ss. 11 to 17.

permission, the telephone company refused to provide information about calls made on the customer's stolen phone after the theft. The victim/customer/police officer contacted the company to enquire why. The company explained its position – it was concerned about protecting the privacy interests (the calling records) of the alleged thief.

Companies do tell police, when they demand a warrant, that they are concerned about being held liable under privacy laws. For those who are concerned about liability and what they perceive to be the legal risks associated with assisting police, normally the only exception they will make is in life and death situations (and even in these situations a few have still refused to provide the non-sensitive customer information they have been requested to provide to police). This is despite the fact that ISPs usually state in their terms of service for customers that if the service is used to break the law they may notify the police. In cases of Internet facilitated child sexual exploitation offences there is no definitive way to assess level of risk to the child until an investigation is undertaken.

If police acquiesce to continued ISP demands for warrants in situations where none are required under the law then their actions will no doubt result in other sectors making requests for warrants prior to cooperating with the police. In cases where an ISP's customer is committing an offence, for example an offence related to child pornography, using the ISP network, at the very least the ISP is a witness.

When investigating known cases of online child exploitation, NCECC members always request customer identifying information from the ISP who holds the IP address and customer identifying information in question. They do so even when the ISP is known to always refuse to voluntarily provide that information to them for the sake of each child/victim who may be a child in need of rescue.

The RCMP, including the NCECC, supports legislative action that would clarify the responsibilities that ISPs have to provide basic customer identifying information to police upon request. Clarifying this obligation in a statute would likely alleviate their concerns over potential liability for disclosing personal information, without an individual's permission and without a court order to authorize the disclosure

5. <u>Time delays, resource impacts, consequences for victims</u>

The NCECC alone makes approximately 200 requests to ISPs per month for customer name and address information. (Data reflecting the level of cooperation from ISPs is documented in more detail below.)[6] All Internet child exploitation (ICE) units make these requests. As already indicated, in many cases obtaining a warrant is not possible or not feasible. Even when it would be possible, the time to complete a warrant, locate and drive to a Justice of the Peace (who is often not in close proximity to the police), wait for the approval, and repeat this process each time another customer's name and address information is needed would place an immense burden on police and court resources across Canada. More importantly, in terms of the potential impact on police, would be

---

[6] See section 8 of this part of the Submission, titled "Statistics supporting the need for legislative response".

the shift in the focus of resources. Finite police resources, previously dedicated to identifying and locating child victims, would now be severely impacted as investigators' already heavy workloads would begin to involve a heavy concentration of time spent on preparing warrant applications and obtaining a court official's approval for their request. In addition, while this shift in utilization of resources would occur, investigators would be cognizant that the abuse of child victims is ongoing. Information they used to reach for in a phone book, or obtain online through a "Canada411" reverse phone number search, or obtain from simply asking a person, is now denied to investigators not because the customer name and address sought is any different, simply because it is deemed to be somehow different.

Recently an online investigator was approached in a public chat room by an unknown person and advised by that person, that he was about to rape his 12 year old step-daughter and broadcast it live. Obviously, in this situation, police did not know where the offender was physically located but instantly were challenged with preventing the assault. To track the suspect's virtual location (indicated by his IP address, the date and time he is online) into a street location, and to try to catch the suspect before he committed the assault, investigators needed to quickly obtain physical address information from the ISP. Without prompt cooperation, not only could the assault occur but the opportunity to ever trace the offender could be forever lost. While police in this situation in Canada would have the grounds to obtain a warrant for the subscriber's address from the ISP, the law does not require police to obtain a warrant for this type of non-sensitive customer information. Furthermore, by the time a warrant could be drafted, taken to a JP and signed the opportunity to locate and rescue the victim could be lost, forever. In this particular case, the offender's IP address belonged to an ISP in the UK. So the investigation was handed off to UK investigators who were able to immediately obtain the customer name and address information that was needed to locate the offender and to rescue his victim.

6. Public expectations of police

The public expects the police to investigate crimes and keep citizens safe. With the exception of the Internet, in every other domain where there is a potential for crime or harm, there exists a capacity for police to rapidly investigate alleged offences. The NCECC believes that the public would support appropriate legislative action to resolve this problem immediately and to ensure that all ISPs are clear about what customer information they may and should provide to police upon request.

Without customer name and address information, an investigation often cannot even begin into child pornography found online and the evidence it points to of the abuse of a child by a potential sex offender. Several studies indicate that between 30 – 75% of all sex offenders who collect and/or possess child sexual abuse images also eventually commit contact offences against children.[7]

---

[7] Hernandez, Andres. (2000). "Self-reported contact sexual offenses by participants in the Federal Bureau of Prisons' sex offender treatment program: Implications for Internet sex offenders." Presented at the 19th Annual Research and Treatment Conference of the Association for the Treatment of Sexual Abusers, San

The inability of ICE Units to begin to investigate many of these reports to determine which of those offenders are currently sexually assaulting children creates a substantial risk for some of the most vulnerable members of Canadian society. A U.S. study on possessors of child sexual abuse images found that the majority (83%) of offenders possessed images depicting children aged 6 to 12 years, and nearly 20% of offenders possessed images depicting children under 3 years of age.[8] Even if it were reasonable to expect these victims to ask for help, this study shows that many victims are too young to call for help. The IP address, captured during the commission of the crime, may be their only possibility for rescue.

An interesting comparison can be made between the tools available to police to respond to a report of a dangerous driver on real-world roads versus a report of a sex offender operating on the virtual highway known as the Internet. NCECC would like to suggest that an IP or email address is similar to a license plate and, therefore, police should have the same immediate capability to identify a person posing a public safety threat on the Internet as they do to identify such a threat on our roadways.

In a report of an impaired driver the primary objective is to intercept the vehicle before death, injury or property damage occurs. If police have license plate information for the suspect vehicle they have instant access to the address of the registered owner of the vehicle.

The registered owner's name does not identify the person in control of the vehicle. It may be stolen, sold or borrowed. The plate itself could be stolen. However, police will attend the location near the last known address of the registered owner and backtrack to the last sighting of the reported vehicle in an attempt to intercept the vehicle before harm is done.

It is NCECC's view that a license plate is similar to an Internet Protocol address. It is only a means to identify the source of a threat and to initiate an investigation. But in online child exploitation cases the IP address is the only means. There is only one source for this information -- a single ISP -- and IP information is perishable as data is purged regularly and often within four hours of online use. The ISP is the only possible source for the name and address of the registered account owner and, like a vehicle, the account holder information will not identify the person operating the Internet account at the time of the offence. Once a starting point is obtained, considerable investigational steps will follow [redacted] Once sufficient evidence exists, a search warrant for the residence

---

Diego, California; Wolak, Janis, Finkelhor, David, and Mitchell, Kimberly J. (2005). "Child-pornography possessors arrested in Internet-related crimes: Findings from the National Juvenile Online Victimization study." National Center for Missing and Exploited Children. Alexandria, VA.

[8] Wolak, Janis, Finkelhor, David, and Mitchell, Kimberly J. (2005). "Child-pornography possessors arrested in Internet-related crimes: Findings from the National Juvenile Online Victimization study." National Center for Missing and Exploited Children. Alexandria, VA.

computer will be requested. If evidence is located during the search, and the perpetrator is identified, then charges can be laid.

7. ISP obligations

All major Canadian ISPs and some smaller ISPs researched by the NCECC have clauses in their customer agreements that prohibit the use of their networks to commit crimes and, often, they further state that they will cooperate with the police. Some explicitly state that if the system is used for child pornography they will cooperate with police. Therefore, it is not contrary to their customers' expectations if they cooperate. Yet they are still reluctant to do so.

ISPs in Canada claim they are simply a conduit and not responsible for the content on their systems or their customers' actions. Nevertheless, the NCECC would suggest that most other businesses expect their customers to act within the law and they take measures to protect their businesses from unlawful activities, so that if their business or their customers are affected by another customer's unlawful actions they can stop it, in collaboration with police.

For example, compare the business of an Internet Service Provider to a restaurant business. Each owner provides a service in exchange for compensation. As with the ISP, the restaurant owner does not care about his customer's personal habits (e.g., if a male customer is with his own wife or someone else's), nor does he care whether that customer is spending his very last dollar there. The restaurant owner must however, ensure that the customer's behaviour does not impact upon the other customers -- if he becomes abusive or obnoxious, the owner would ask him to leave. He must ensure that the customer is not over-served alcohol and if he appears to be intoxicated, the owner will ensure that he does not drive away by calling a taxi or the police. If the customer commits other crimes such as failing to pay for the meal, or attempts to use a stolen credit card, or starts a fist fight with someone in the restaurant, one can be fairly certain the restaurant owner would call police and would assist the police in identifying the customer. If police arrived unexpectedly and advised that a previous customer was suspected in the sexual assault of a child, the restaurant owner would provide all assistance possible. Somehow the reality of the child at risk seems to impact the restaurant owner far more than some ISPs.

In contrast, an ISP's customer may prey on children by luring, grooming or extorting them; send them live broadcasts of his masturbation; sexually assault children and share the sexual abuse images online; promote adult-child sex. Yet, unlike the restaurant owner who understands the link between what is happening on his premises and real crime and will call police if a problem arises, some ISPs apparently are neither on the look-out for crimes that may be occurring there nor do they report crime detected on their facilities. RCMP records show that the RCMP has only ever received one report of suspected online child exploitation from an ISP. Furthermore, when an ISP is approached by police regarding illegal activity involving a customer/ sex offender, who is using its

network or services, and when the ISP is asked to assist in many instances, as already discussed, such requests are being refused.

It may be that part of the explanation for the differences noted here is that ISPs are not a heavily regulated sector in comparison to food services which are well-regulated. However, from a policing perspective, rules (in the form of legislation) are needed to clarify for all ISPs and other telecommunications service providers that certain customer identifying information must be provided to police upon request, in the interest of public safety.

8. Statistics supporting the need for legislative response

Statistics for the number of telephone and Internet company refusals to provide basic customer identifying information is not being collected across all sectors of policing operations. Currently, only the NCECC is collecting this data. Since CCAICE instituted the current administrative model NCECC has had some success obtaining certain customer information from certain ISPs. However, this model is only used in cases of Internet facilitated child exploitation. Consequently, the RCMP is confident the percentage of refusals, if they were recorded in other areas of RCMP operations, would be even higher than the percentage of refusals that NCECC has noted. .

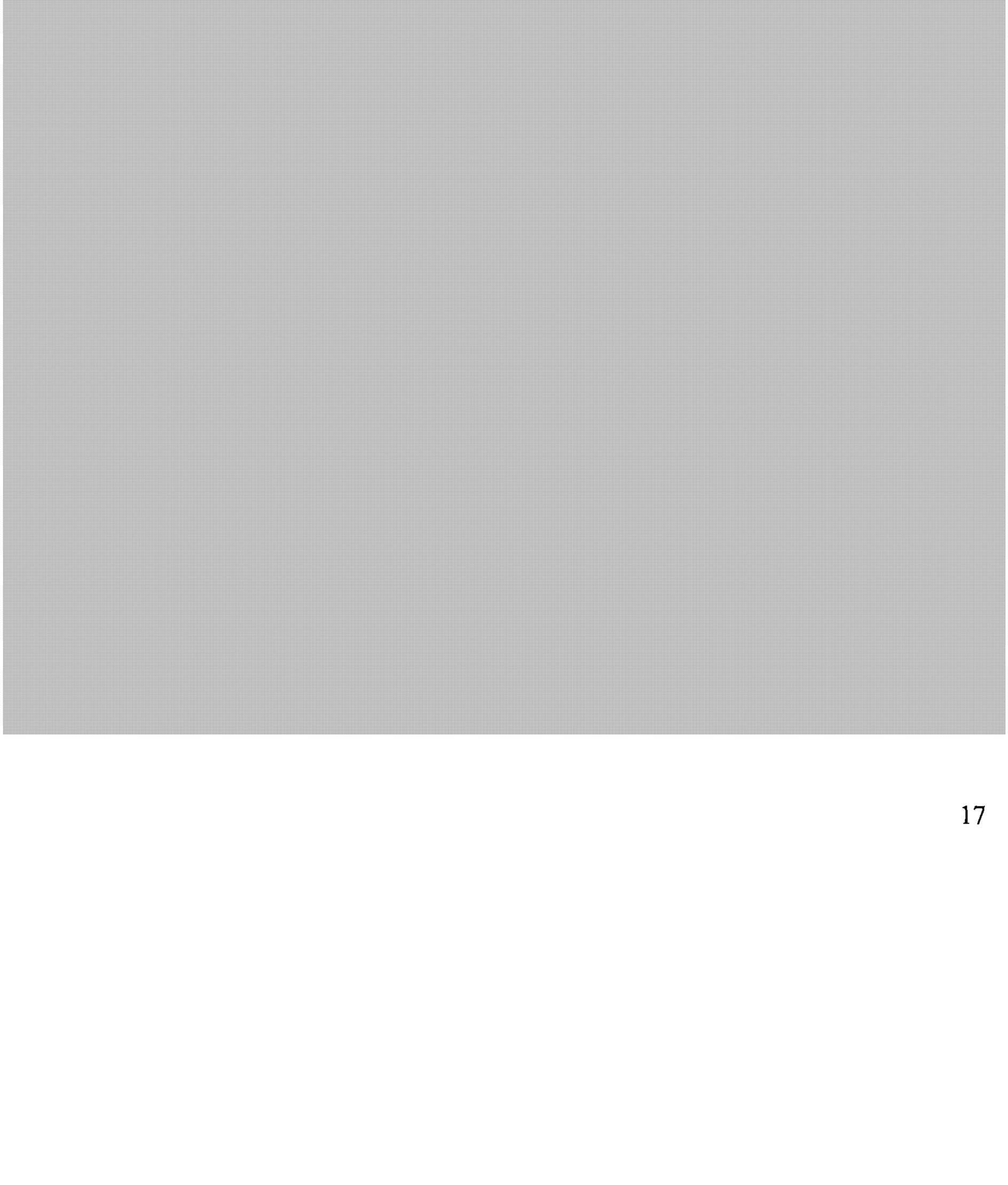
Results vary from this voluntary administrative process, whereby Internet child exploitation (ICE) investigators can request CNA information from ISPs , but the average over the past six months is that 33% of NCECC requests produce unsuccessful results. One third of all leads are concluded without investigation. The reasons are documented as refusals, lack of response or insufficient data retention times. The NCECC has now asked all major ICE units from BC, Alberta, Manitoba, Quebec, Ontario, Nova Scotia and New Brunswick to begin to log this data and to provide NCECC with their results.

NCECC Statistics for Customer Name and Address Requests and Results

2007 NCECC Requests	**ISP Response Summary**
March	***44% non-compliance***
April	384 requests made 164 refusals ***42% non-compliance***
May	***33% non-compliance***
June	125 requests 27 refusals ***21% non-compliance***
July	49 requests 16 refusals ***32% non-compliance***

August	62 requests 17 refusals ***27% non-compliance***

Specific Examples from International Cases



[redacted]

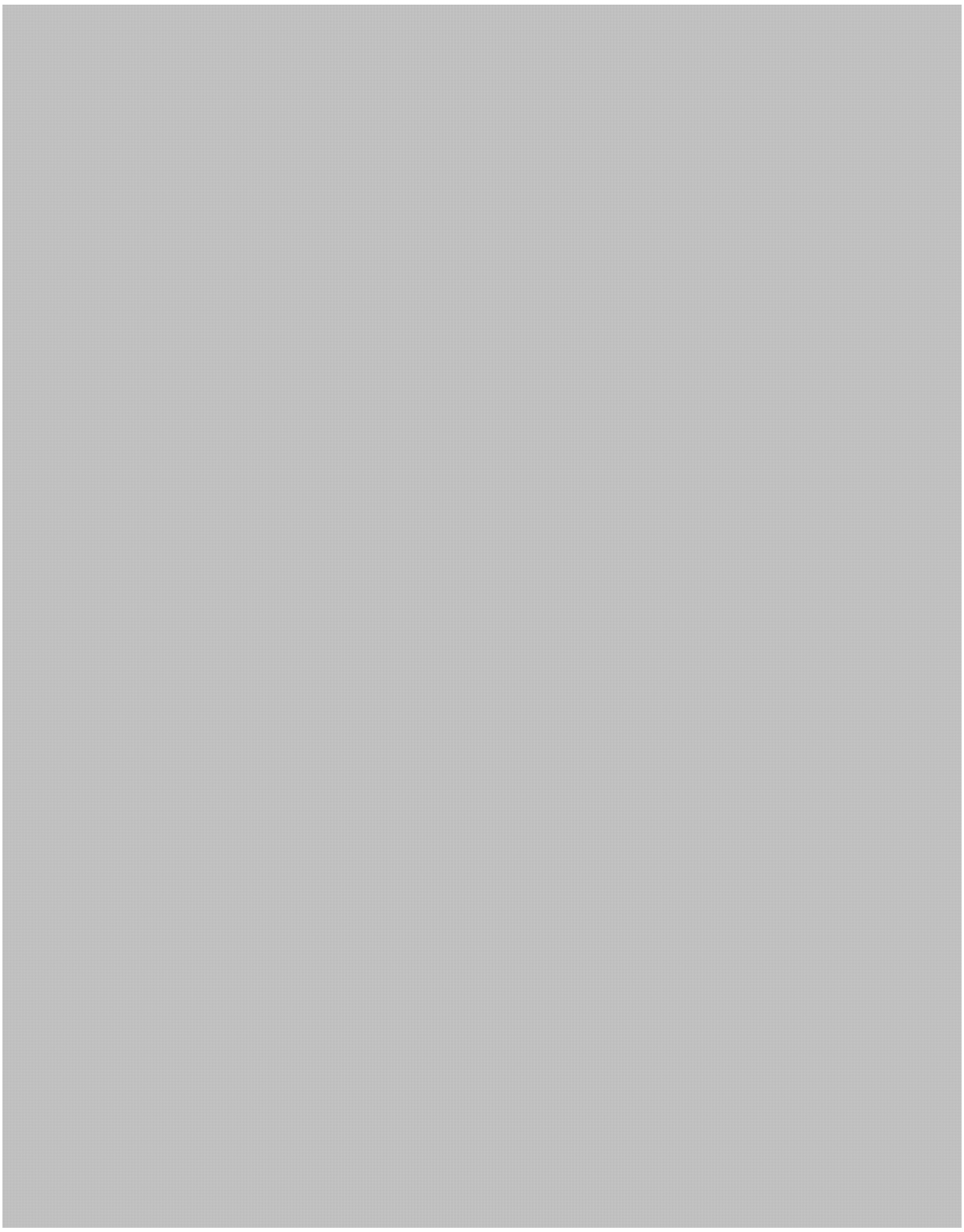
9. Public support for police efforts

The NCECC believes that if the Canadian public had fuller knowledge of the challenges police are facing obtaining basic customer identifying information from ISPs, and the potential effect an ISP's refusal can have on effective law enforcement, the overwhelming majority of Canadians would be fully supportive of legislative proposals that would compel telecommunications service providers to provide this information to police, subject to reasonable privacy safeguards.

The NCECC is concerned that inaccurate and negative portrayal of the "customer name and address" issue in some media reports has left Canadians with a distorted view of the legislative proposals. The proposals would not compel telecommunications services providers to give police sensitive personal information without a warrant. Police are not seeking to obtain information without a warrant, where a warrant is normally required. That information would not be admissible in court and therefore useless to investigators.

The RCMP notes that Public Safety Canada's "Customer Name and Address Consultation Document" indicated that "options based on an administrative model are being considered" and it proposed that "a number of safeguards could be included under a possible administrative model requiring the release of limited basic CNA information to law enforcement". The RCMP supports the proposal for an administrative model, based in legislation that would include provisions to safeguard the privacy of this customer information and protect it from misuse. The RCMP hopes that with broader and more transparent consultations, the public debate may become more informed and the public criticism may decrease. The RCMP believes with a greater appreciation for the CNA

issue and the proposed legislative solution, a majority of the public would support these proposals.



Pages 201 to / à 203

are withheld pursuant to section

sont retenues en vertu de l'article

21(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

International Perspectives

Ms. Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management & National Security
Public Safety Canada
16C, 269 Laurier Ave. W.,
Ottawa ON, K1A 0P8

Thursday, October 4th, 2007

Dear Ms. Clairmont,

Thank you for the invitation to participate in consultations regarding an important security measure, Lawful Access. I have avidly followed the subject both in Canada and internationally for a number of years and am happy to provide some thoughts on current endeavours to implement a Canadian Lawful Access measure.

Lawful Access legislation is a critical security measure. The ability to intercept communications enables law enforcement agencies to gain valuable insight and evidence with which to build cases around suspected criminals. Many countries have opted to update existing or implement new measures as a result of the widespread use of emerging communication technologies. Canada is one of a few countries that has not enacted separate regulations around Lawful Access (LA). The chief reason why such important legislation has to date not been enacted stems from a failure to build consensus among key stakeholders as to what shape such LA legislation and, ultimately, regulations should take.

Central to this absence of consensus has been a lack of disclosure of statistics around past and current uses of wiretapping and release of Customer Name and Address (CNA) information as investigative tools. In fact, little to no statistical data covering any aspect of LA, as it is currently used, that can support the need to implement a new bill or enhance existing provisions has been publicly provided. This lack of disclosure not only renders draft LA measures baseless, but also causes much distrust among key stakeholders outside of the law enforcement realm.

Collecting and analysing data around the current use of LA provides a solid understanding for how a new security measure should be created. Such statistics indicate how useful the measure has been to date, which in turn can quantify exactly what sort of resources should be allocated to enhancing provisions and what those enhancements should be. For example, statistics might indicate that due to emerging communications technologies the costs associated with enhancing

interception capabilities on some internet-based services is far greater than the benefits to society of such enhancements. As a result, resources may be better allocated to developing innovative policing methods that answer the changing realities of modern investigations. Conversely, statistics may indicate that the measure is exceptionally useful and provide a clear picture of how best to move forward based on legitimate evidence acceptable to all key stake-holders.

Without statistics around the current use of LA as a basis for provision enhancements any attempts to push through a new measure will certainly be met with widespread disapproval. It is conceivable that basing a security measure, such as LA, on the requests of law enforcement in the absence of supporting data can negatively impact the image of respect held by police among the Canadian public. This is especially true at a time when one of our federal law enforcement agencies is increasingly scrutinised as a result of corruption allegations

While no one doubts the need of law enforcement in Canada, it must be remembered that even those entrusted to uphold the law require oversight. The human factor must be taken into account. It should not be inconceivable that there remains the potential for abuse of a tool such as wiretapping. Such abuse might include corrupt police officers abetting criminal organizations or a frustrated investigator abusing poorly regulated privileges to gather information on a suspect where official channels have failed. Providing statistics around the current use of LA in Canada would assist in quelling such concerns held by privacy advocates. Furthermore the provision of statistics would help engage privacy advocates in creating a measure that benefits society.

From a security perspective, introducing a security measure without supporting data risks the stability of the entire governing system. As the stability of our society depends upon the symbio-sis between civil society and law enforcement, any actions that jeopardise the necessary respect for and co-operation with Canadian police among the general public have the potential to nega-tively impact the wider system in the long run. Despite a seeming readiness among Canadians to forgo certain civil liberties in the name of security, measures enacted without foundation risk eroding such faith in leadership, particularly when those measures strengthen the *perception* of enhanced security as opposed to actually *making* Canada more secure. Indeed, Canadians have proven to have a surprisingly low threshold for tolerating security measures that fail to protect the best interests of citizens (consider, for example, the incident in Grand Manan, New Brunswick during the summer of 2006.) Using a scientific approach in implementing new LA legislation will ensure that the respect currently enjoyed by law enforcement in Canada is continued well into the future.

Statistics on the current use of LA also provide much needed insight as to what the technical scope of enhancements to existing provisions should be. The costs of implementing new

P www.internationalperspectives.org 1.416.566.8717
info@internationalperspectives.org

technology to comply with LA legislation can be considerable. Supporting data can assist in developing regulations and parameters for enhancing LA provisions thus providing a well-defined scope and targets which industry can then meet. In the absence of supporting data and analysis, any plans to enhance existing LA provisions will be carried out blindly. After all, it is impossible to determine scope without first understanding what reasonable and efficient technical enhancements are actually needed. Without a clear, well-founded plan as to how LA enhancements will be carried out, it should be anticipated that industry would view attempts to pass a measure unfavourably.

Considering these different angles, I strongly recommend that basic information regarding the current use of LA be immediately collected and analysed before any further attempts at implementing a measure be carried out. At a minimum, the following information should be collected over an appropriate period (perhaps six (6) months or as long as required in a given sector), while at the same time preparing a basic framework for the new measure as incoming data indicates scope:

- The number of times wiretapping or requests for CNA information are being made, broken down by requesting organization as well as type of request;

- Whether the request for a warrant or CNA information was refused and why;

- The nature of the crime or circumstance why such requests are being made;

- Type of communication technology to be intercepted and whether or not the surveillance attempt was successful; &

- Direct correlation as to the usefulness of the request with closing the investigation as well as prosecution of the target.

To ensure the integrity of the data collected, both law enforcement agencies as well as counterparts inside of CSPs should be mandated to collect the above information. The data retention process could be as simple as completing and submitting an official form, thus enabling an almost immediate implementation of the reporting mechanism.

A small committee of individuals, each representing a respective key stakeholder, should be set up at arm's length to analyse the data and put forth findings and recommendations for moving forward. Such a reporting process should continue on a permanent basis to ensure accountability of measures such as LA.

With a proper approach it is possible to enact a measure efficiently that protects civil liberties as well as facilitates law enforcement without over burdening industry. Such a balance, however, can only occur if the measure is based on supporting statistics and all perspectives are considered equally in the drafting of such a bill. I believe that the above recommendations will assist the government in achieving the necessary balance while also enacting an effective long-term measure.

Should you have any questions regarding the thoughts presented in this letter or need clarification, please do not hesitate in contacting me.

Sincerely,

Executive Director
International Perspectives
1.416.556.8717
awanless@internationalperspectives.org

TED ROGERS SCHOOL OF MANAGEMENT
RYERSON UNIVERSITY

Dr. Avner Levin
Director, Privacy and Cyber Crime Institute
Chair, Law and Business Department

October 8, 2007

Ms. Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Re: CNA Information Consultation

Dear Ms. Clairmont,

Thank you for inviting me to participate in the CNA Information Consultation. I am pleased to provide my comments on the Consultation Document in this letter. These comments are based significantly on the public reassurances made by Minister Day during recent media appearances, in which the Minister appears to have stated that the proposed legislation will not provide Law Enforcement Agencies (LEAs) with the power to lawfully access CNA information without a warrant. I support the Minister's position and view it as at the right approach to take at the present time.

It is important to note that my support for the Minister's present position is not based on a "knee-jerk" reaction to the Consultation Document. I agree wholeheartedly with the concerns of LEAs about increased terrorism and national security risks, as well as their concerns about cyber-crime in general. I agree as well to the need to ensure the cooperation of TSPs in emergency situations, such as recent well-publicized cyber child molestation incidents.

Unfortunately, I have yet to see empirical evidence of the difficulties that LEAs claim to have experienced in obtaining CNA information from TSPs. I would urge Public Safety to request such information from LEAs. It would be useful for LEA supporters to have at their disposal statistics that detail investigations that have been hampered by the judicial oversight currently in place, especially since privacy advocates voice the concern that warrants are often issued with little scrutiny of LEAs. Police investigators often state in public appearances the technological difficulties of a modern cyber forensic investigation, or the legal difficulties of international investigation and extradition treaties, which do indeed need to be streamlined to allow for efficient and swift procedures. I do not recall however a case in which LEAs identified a TSP that refused to cooperate (voluntarily) in a situation where an individual was threatened or molested, or where cyber-criminals, let alone terrorists, were not brought to justice because of the reluctance of the judicial system to issue warrants.

I believe that the Canadian public would strongly support access to CNA information in emergency situations, and generally without judicial warrants, if presented with such unequivocal statistical evidence. I also believe that the Canadian public and the present Federal Government are quite sensible in retaining the present judicial oversight mechanism in place as long as there is no such demonstrated need. I would be happy to continue and participate in a CNA consultation on the merits of an administrative model once LEAs have made the empirical case for their requests.

Sincerely,

(-)

Avner Levin

575 Bay Street, Toronto, Ontario M5G 2C5 (entrance) 55 Dundas Street West
Tel: 416-979-5121 Fax: 416-979-5266 www.ryerson.ca/tedrogersschool/

CARL ABRC

Canadian Association of Research Libraries

Association des bibliothèques de recherche du Canada

October 9, 2007

Customer Name and Address Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa ON K1A0P8

VIA EMAIL: cna-consultations@ps-sp.gc.ca

Dear Sir/Madam,

Re: Lawful Access

The Canadian Association of Research Libraries (CARL) is the leadership organization for the Canadian research library community. The Association was established in 1976: CARL is an affiliate member of the Association of Universities and Colleges of Canada (AUCC) and is incorporated as a non-profit organization under the *Canada Corporations Act*.

CARL has an ongoing interest in legislation relating to lawful access to information by law enforcement officials. CARL therefore welcomes the opportunity to provide policy makers with a description of the potential implications of legislation for CARL member libraries. On review, these implications are similar to those expressed regarding Bill C-74, the *Modernization of Investigative Techniques Act* (MITA). With the dissolution of the House of Commons in 2005 this Bill died on the order paper.

1. Cost Implications
There are two types of costs associated with lawful access legislation for CARL member libraries. The first is infrastructure requirements related to changes to existing systems and networks. The second cost implication pertains to library operations. It is difficult to know how substantial these costs may be without concrete legislative proposals. Cost nevertheless is a concern for CARL members.

2. Distinguishing Data Retention and Preservation
Data retention and data preservation must be distinguished in the drafting of any legislation. Bill C-74 proposed that a data preservation order would require a service provider to keep existing data of a specific individual identified by the courts as the subject of an investigation and not delete it for a specified period of time. Data retention, on the other hand, involves the collection of data from all users of a communication service - regardless of whether or not they are subject to an investigation. The latter would create an administrative burden on our membership for no defined purpose.

Canadian Association of Research Libraries /
Association des bibliothèques de recherche du Canada
Room / Pièce 239, Pavilion Morisset Hall, 65 rue University Street
Ottawa Ontario K1N 9A5

613.562.5385
613.562.5195
carlabrc@uottawa.ca
www.carl-abrc.ca

3. Judicial Authority Requirement
Lawful access legislation must not provide undue discretionary authority to law enforcement officials to seek out and seize information. This is the same concept that underlies current access provisions, such as those governing search warrants and wiretaps. There must continue to be legal checks in place to ensure that law enforcement officials gain access only when they have just cause, and have appropriate judicial authorization. This concern is founded in part on the experience of our colleagues in the Unites States in dealing with the demands under the *Patriot Act.* Libraries should remain a place where individuals are free to pursue their studies without fear that they could lead to prosecution.

4. Privacy
"Lawful access" to electronic information by law enforcement officials must provide appropriate safeguards to protect privacy rights of those engaged in typical library activities. There is a need to balance lawful access requirements with privacy rights guaranteed by the Charter of Rights and Freedoms and other legislation. The privacy rights of the individuals in CARL member institutions must be balanced with the requirements of law enforcement officials to track and prosecute criminals. Some invasion of individual privacy is justifiable in the interest of protecting society as a whole from criminal activity. CARL will review any proposed lawful access legislation to determine whether it strikes the appropriate balance between these two competing public policy objectives.

5. Defining "Prescribed Information"
The information that will be required to be provided to law enforcement officials as "prescribed information" must be carefully defined. CARL will have to see what is included as "prescribed information" in order to assess whether the information to be covered by the definition has been appropriately defined. Ministerial discretion to require significant reporting requirements should be avoided.

Thank you for your consideration of the above points.

Yours sincerely,

Leslie Weir (Ms)
President

cc. Mr. William Maes, Chair, CARL Government Policies and Legislation Committee
Mr. Timothy Mark, Executive Director, CARL

Federal Ombudsman for Victims of Crime Submission to the CNA Data Consultation Panel

October 10, 2007
Ottawa, Canada

FEDERAL OMBUDSMAN FOR VICTIMS OF CRIME
SUBMISSION TO CNA DATA CONSULTATION

The Office of the Federal Ombudsman for Victims of Crime was announced in March, 2006 by the Minister of Justice and the Minister of Public Safety. The mandate of the Federal Ombudsman for Victims of Crime relates exclusively to matters of federal responsibility and includes:

- facilitate access of victims to existing federal programs and services by providing them with information and referrals;
- address complaints of victims about compliance with the provisions of the *Corrections and Conditional Release Act (CCRA)* that apply to victims of offenders under federal supervision and provide an independent resource for those victims;
- enhance awareness among criminal justice personnel and policy makers of the needs and concerns of victims and the applicable laws that benefit victims of crime, including to promote the principles set out in the *Canadian Statement of Basic Principles of Justice for Victims of Crime*; and
- identify emerging issues and exploring systemic issues that impact negatively on victims of crime.

As part of our duty to alert the Government to emerging issues that impact negatively on victims of crime, we identified Internet facilitated child sexual exploitation as one of our main priorities. Despite the many positive aspects of the Internet for children, it has had a significant negative impact on some child victims of sexual abuse. We agree with the federal government that more needs to be done to identify and rescue children from ongoing sexual abuse and to prosecute those responsible for exploiting them.

The ability of police to identify and rescue children and to prosecute predators is essential. Many Internet Service Providers (ISPs) do cooperate with requests for information when police provide a letter of request. But according to the RCMP's

National Child Exploitation Coordination Centre, 30-40% of requests are denied. That means many predators go undetected, and many children are potentially left in abusive situations.

THE IMPACT OF INTERNET FACILITATED CHILD SEXUAL ABUSE

There are over 1 million child sexual abuse images on the Internet. Twenty thousand new pictures are added every week.[1] There are over 100,000 searches daily. There are tens of thousands of websites that promote sex with children.

The children seen in the images are getting younger and the abusers are getting more violent.[2] Over 85% of the children are under 12, many under 9 and almost one in five are under 3.[3] Eighty percent of the images involve penetration and 20% involve torture or bondage.[4]

Eighty percent of the abuse seen online is committed by people the children know.[5] Many of those who access and trade images are also abusers themselves. One study in the US found that 80% of offenders in prison for child pornography-related offences admitted to being abusers.[6]

---

[1] Unless otherwise stated, the statistics are provided by the RCMP's National Child Exploitation Coordination Centre.
[2] OPP Detective Inspector Angie Howe, *Senate Legal and Constitutional Affairs Committee*, Bill C-2, June 22, 2005.
[3] http://www.mg.co.za/articlePage.aspx?articleid=320210&area=/insight/insight__international/
[4] CTV.ca, July 23, 2006.
[5] C-CAICE
[6] Dr. Peter Collins, *Standing Committee on Justice and Human*, Bill C-2, May 3, 2005.

Therapists, law enforcement and victim services have years of experience dealing with child sexual abuse victims, but there is growing recognition that child sexual abuse images and the Internet complicate the impact of the offences, the recovery of victims and the delivery of services. Tink Palmer, a member of *Stop it Now! UK*, asserts that, "…we need a radical reconsideration of current practices, policies and procedures in the light of new technological conduits for abusing children."[7]

She goes on to say, "the additional trauma for a child who knows that their humiliation has been photographed or filmed, and that people around the world may access and witness it in the immediate present and also long into the future, has serious and complex implications for assisting the child's recovery and for the way such crimes are investigated."[8]

End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes' (ECPAT) contends, "Child pornography amplifies and broadcasts the original act of abuse that it depicts. In doing so, it can substantially aggravate the original offence."[9]

One child sexual abuse victims whose photos were put on the Internet said, "Usually, when a kid is hurt and the abuser goes to prison, the abuse is over. But because XXX put

---

[7] Tink Palmer, "Abusive images: The impact on the child," in ECPAT Newsletter, Issue 49 1/January/2005.
[8] Tink Palmer, "Abusive images: The impact on the child," in ECPAT Newsletter, Issue 49 1/January/2005.
[9] John Carr, "Theme Paper on Child Pornography for the 2nd World Congress on Commercial Sexual Exploitation of Children" p.13
http://www.ecpat.net/eng/Ecpat_inter/projects/monitoring/wc2/yokohama_theme_child_pornography.pdf

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."[10]

Another victim said, "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."[11]

The Supreme Court of Canada, in the case of *R. v. John Robin Sharpe*, said,

> "The child is traumatized by being used as a sexual object in the course of making the pornography. The child may be sexually abused and degraded. The trauma and violation of dignity may stay with the child as long as he or she lives…the child must live in the years that follow with the knowledge that the degrading photo or film may still exist, and may at any moment be being watched and enjoyed by someone."[12]

Victims often do not disclose that photos were taken or videos were made, and even when confronted with such discoveries, some victims will refuse to acknowledge that this was done. "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…Anxiety may intensify where a child understands that images of their abuse will continue to be replicated and circulated to an audience that is both nearby and global long into the future."[13]

---

[10] Julian Sher, *One Child at a Time*, 2007
[11] Julian Sher, *One Child at a Time*, 2007
[12] R. v. Sharpe, [2001] 1 S.C.R. 45, 2001 SCC 2, paragraph 92.
[13] ECPAT International, "Violence Against Children in Cyberspace," 2005. p.41

Children may have difficulties accepting that they cannot control their images; that once they are on the Internet, men around the world may be using them for their own sexual gratification or to groom other children. They must learn to live with the reality that their photos will be on the net and in people's computers forever. ECPAT says,

> "...even where it has been possible to identify a victim, the chances of being able to help the child to recover from the trauma of the initial involvement in the abuse can be seriously compromised if the child learns or comes to believe that images of them engaged in the abusive behaviour might have been scanned, or converted into a digital format in some other way, for storage on a computer or for transmission between computers e.g. over the Internet. This, in effect, makes the image part of a permanent public record. It could, even randomly, suddenly appear on the screen of their next-door neighbour or classmates."[14]

FEDERAL GOVERNMENT'S COMMITMENT TO CHILDREN

There can be little doubt that this Government has repeatedly displayed its commitment to protect children from those who would prey on them. Bill C-22, which would raise the age of consent from 14 to 16, is but one example.

That commitment was also evident in the 2007 Budget, when the Minister of Finance gave an additional $6 million to the RCMP to protect children from sexual exploitation. Minister Flaherty said, "The funding will ensure that those who commit these heinous offences are brought to justice..."

In 2003, the Government of Canada signed the *Canadian Basic Statement of Principles for Victims of Crime*, which commits the federal government to consider and respect the

---

[14] John Carr, "Theme Paper on Child Pornography for the 2nd World Congress on Commercial Sexual Exploitation of Children" p.14
http://www.ecpat.net/eng/Ecpat_inter/projects/monitoring/wc2/yokohama_theme_child_pornography.pdf

privacy of victims to the greatest extent possible; to minimize inconvenience to victims and to take appropriate measures to protect victims. Canada is also a signatory to several key UN declarations that speak to the need to protect and promote the safety and privacy of victims and children.

More recently, Canada with other G8 Ministers agreed to accelerate efforts to combat child sexual exploitation. The G-8 Ministers committed, "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."[15] The Ministers also acknowledged and recognized that the private sector, including Internet Service Providers (ISPs), have a role to play in protecting the world's children." The Ministers recognized that, "Child pornography grievously harms all children: it harms the child who is sexually assaulted in the making of the image; the same child is re-victimized every time that image is viewed."[16]

THE LAWFUL ACCESS DEBATE

For years, the law enforcement community has been calling upon the federal government to reform the *Criminal Code* to enable them to apply real world police tools to the virtual world. For example, police can get a customer's name from a telephone company, but not from an Internet Service Provider (ISP). After a series of consultations, the former government introduced Bill C-74, which among other things (that will not be discussed

[15] G-8 Justice and Home Affairs Ministers, May 24, 2007. www.g8.gc.ca/childpornography-en.asp
[16] G-8 Justice and Home Affairs Ministers, May 24, 2007. www.g8.gc.ca/childpornography-en.asp

here in any detail) enhanced law enforcement's capability to access customer name and address (CNA) information from ISPs. Although the bill had problems,[17] it was seen as a welcome initiative by those concerned with law enforcement and the protection of children from Internet sexual predators. Bill C-74 died on the Order Paper when the election was called.

Subsection 7(3)(c) of the *Personal Information Protection and Electronic Documents Act (PIPEDA)* sets out provisions where an organization **may** disclose personal information without consent. It refers 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.

Parliament clearly intended to facilitate the enforcement of criminal law, but the Committee heard that law enforcement has found it to be a hindrance. Of particular concern is with respect to investigations of suspected Internet facilitated child sexual exploitation. Some ISPs do cooperate with law enforcement requests in child sexual abuse investigations, in part because they recognize the uniqueness of the child pornography[18] provisions in the *Criminal Code* - that it is a crime to simply access and view child sexual abuse images. That makes it somewhat different than other crimes. For

---

[17] For example, the bill allowed companies exceptions if it was cost prohibitive. This is not consistent with other industries. Government does not allow the car industry to only take safety measures if they can afford it. When municipalities impose smoking bans on restaurants and establishments, there are no exceptions for establishments that might suffer a financial hardship.

[18] Generally, we prefer to use the term child sexual abuse images (CSAI) rather than child pornography because CSAI is more reflective of what it is we are talking about – permanent records of child abuse. We a woman is raped, we do not call it adult pornography. We should not do it when it comes to children.

example, it is not illegal simply to read hate literature. Unfortunately, not all ISPs cooperate with law enforcement.

The Standing Committee on the Access to Information, Privacy and Ethics conducted a widespread review of the *Personal Information Protection and Electronic Documents Act (PIPEDA)* during the last year. It released its Fourth Report earlier this year.

Mr. Clayton Pecknold of the Canadian Association of Chiefs of Police testified before the Committee and explained the challenges the police currently 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). (February 13, 2007)

On August 16, 2007, I wrote to the Honourable Jim Prentice, Minister of Industry, in relation to *Recommendation #12* of the Committee's Report, which is relevant to this consultation as it reflects the will of the committee and was a unanimous recommendation, indicating support for the recommendation from all parties. The recommendation states,

> *"The Committee recommends 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 [...]"*

The Committee agreed that it is not realistic or necessary to expect police to seek a warrant in these situations. By including subsection 7(3)(c.1), Parliament clearly did not intend for law enforcement to secure a warrant for information that is not considered personal.

IS CNA PERSONAL INFORMATION?

Recently, the Federal Court ruled that EBay had to give personal information about high volume sellers' clients to the Canada Revenue Agency in order to ensure that those individuals are paying the appropriate taxes.[19]

Courts have said that people do not have a reasonable expectation of privacy attributed to their name and address. In *R v. Plant,*[20] 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 thc 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."[21]

The Court of Queen's Bench of Alberta said, "thcrc is no reasonable expectation of privacy with respect to: 1. General banking information - see *R.* v. *Lillico* (1994), 92

---

[19] Paul Waldie, Taxman goes browsing on eBay, Globe and Mail, September 27, 2007
[20] *R. v. Plant*, [1993] 3 S.C.R. 281. This case dealt with marijuana grow-ops and the police obtained information from the electricity company regarding the owner's electricity use.
[21] R. *v.* Plant, [1993] 3 S.C.R. 281

C.C.C. (3d) 90 (Ont. Gen Div.); [1999] O.J. No. 95 (Ont. C.A.); 2. Cellular telephone records - see *R.* v. *Brown,* [2000] O.J. No. 1177 (Sup. Ct. Jus.) at para.63."[22]

In *R. v. Quinn,* in which police requested "tombstone" information regarding several accounts in which cheques had been deposited, the BC Court of Appeal said, "there was no search, much less any unreasonable search as envisioned in the *Charter.*"[23]

If EBay has to give the Canada Revenue Agency the names and addresses of citizens to make sure that taxes are paid, does it not seem strange that Internet Service Providers (ISP) do not have to give the same information to the police trying to find a sexual predator who may be abusing a child? Measures to prevent a predator from abusing a child should be given the same priority as collecting unpaid taxes.

This is not a privacy issue. It is a public safety issue. It is a child safety issue.

Some have suggested that police should be required to get a warrant for this information. This is inconsistent with the view of the courts which have said this kind of information is not personal. This is, after all, information that can be found with a license plate, phone book or driver's license. The reality of Internet facilitated child exploitation investigations is that children may be at immediate risk. Most abusers seen in online abuse images know the child; many are related; and therefore they have ongoing access to the child.

---

[22] *R. v. Haskell*, 2004 ABQB 474
[23] *R. v. Quinn* 2006 BCCA 255 paragraph 93

In 2004, Michael Briere murdered 10 year old Holly Jones minutes after looking at child sexual abuse images online. He walked out of his home and saw the young girl walking down the street. He grabbed her, took her into his home where he sexually assaulted her before killing her and taking steps to dispose of her remains. At his sentencing hearing, Briere told the court he was consumed by desire after viewing child pornography.[24] While this is an extreme example of what can happen, it should be an important reminder to all of us. Law enforcement officers are increasingly seeing children being abused live on the Internet. And none of us know what happens when the predator turns the computer off. He might not do what Michael Briere did, but it is not a leap of logic to suggest a child might be at risk of further abuse.

It is not acceptable to demand law enforcement to waste their valuable time and resources, not to mention the court's time and resources, to get a warrant for information that the Canada Revenue Agency can demand from EBay. This is information they can demand of someone they see jaywalking or through the license plate of someone seen driving away from a car accident. Preventing child sexual abuse and tracking abusers is as important as preventing traffic accidents and enforcing street laws.

The suggestion that law enforcement secure a warrant for CNA assumes law enforcement can get a warrant in these circumstances, which may not be the case. It is not a question of inconvenience or making a police officer's job easier; it is about rescuing children.

---

[24] CBC News Online, http://www.cbc.ca/news/background/jones_holly/

The government's Consultation Paper says, "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.*"

The good news is that many ISPs are cooperating with police without a warrant, although it remains to be seen what the impact of the Minister's recent comments will be on those companies.

The bad news is requests are denied 30 to 40% of the time.[25] That means 30% of investigations might end on the starting block, and children at risk are left in those abusive situations. Even if the number was lower, it still would not be acceptable. It is unacceptable that we leave a child in an abusive situation one day longer than necessary. Those children must not be sacrificed for the misplaced concern for individual privacy.

The recent debate has created the perception that police want more than just CNA; that they want access to emails. It has also left people with the mistaken belief that police can easily get a warrant in these circumstances. The reality is quite different.

This is what law enforcement refer to as the pre-warrant stage. It is the beginning of an investigation and they need a name to begin the investigation. If they get a name and find out, for example, that John Doe has a 5 year old girl who matches the description of the

[25] RCMP's National Child Exploitation Coordination Centre

images they found online, then they might knock on John's door and save that little girl from being raped that night. But if they cannot get John Doe's name and address, they will not rescue that child.

It is important to note that getting CNA does not mean that the customer is the perpetrator. It does not place him/her in front of the computer at the time the images were traded (for example). An investigation will be required to determine that. But again, it begins with a name and address.

Other countries, including the UK, Australia and the US, do not require law enforcement to secure a warrant before accessing CNA from an ISP. In fact, the scheme set out in Bill C-74 appeared to be more restrictive than that of the other three countries."[26]

WHAT ABOUT THE PRIVACY OF THE CHILD?

At the risk of being repetitive, this is not a privacy issue but a child safety issue. It is unfortunate, given that the debate has focused so much on privacy, that not one word has been spoken about the privacy interests of the children whose images are being traded like baseball cards. The *Canadian Statement of Basic Principles of Justice for Victims of Crime* requires the federal government to consider the privacy interests of victims.

---

[26] Dominique Valiquet, Telecommunications and Lawful Access: II. The Legislative Situation in the United States, the United Kingdom and Australia, 28 February 2006, Library of Parliament, http://www.parl.gc.ca/information/library/PRBpubs/prb0566-e.html.

The Supreme Court said,

> "Child pornography also undermines children's right to life, liberty and security of the person as guaranteed by s.7....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."[27]

Is there any more serious privacy violation than to allow images of a child being raped to be distributed to hundreds of thousands of sexual predators? Imagine growing up knowing those photos are available forever, for anyone to see, and you have no control over them. It should put the controversy over releasing a name in perspective.

CONCLUSION

This debate is not about increasing police powers or the Government's ability to monitor people's activity on the web. It is about rescuing children from potentially abusive situations and prosecuting those who might be abusing and exploiting them.

Everyday, police officers across the country sit in front of computers and sift through tens of thousands of images and watch videos of the most horrific abuse imaginable. They hear the screams of pain. They see the tears.

---

[27] R. v. Sharpe, [2001] 1 S.C.R. 45, 2001 SCC 2, paragraph 189.

If society is going to ask them to do this work, they need to give them the tools to finish the job. Not for the police, not to make their job easier, but for the children.

During a presentation at the NCECC/OPP recent conference, a short audio clip of a little girl being raped by her father.[28] She said, "Daddy, it hurts. It hurts so bad."

What if police needed CNA to help find her but the ISP said no and they could not get a warrant? It is unspeakable that a father would do that to his child, but it would be unforgivable if he was allowed to do it again.

[28] The presenter was illustrating how new software can be used to enhance sound.

RECOMMENDATIONS:

As Federal Ombudsman for Victims of Crime, I recommend the federal government enact legislation requiring ISPs to provide CNA information to law enforcement investigating Internet facilitated child sexual abuse cases. Legislation is necessary to clarify that a judicial authorization is not necessary and that the current practice in which many ISPs accept written requests for CNA from authorized law enforcement officers investigating Internet facilitated child sexual abuse be adopted.

Furthermore, in addition to audit results being provided to the Privacy Commissioner (as was proposed in the consultation document), I recommend that audit results also be provided to the Federal Ombudsman for Victims of Crime.

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.

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 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 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.

---

[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

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]

It is the term *lawful authority* that is problematic. 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

[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;"

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

Information and Privacy Commissioner/Ontario
Commissaire à l'Information et à la protection de la vie privée/Ontario

October 10, 2007

The Honourable Stockwell Day
Minister of Public Safety
Care of Customer Name and Address Information Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, Ontario
K1A OP8

Dear Minister:

RE: 2007 Lawful Access ("Customer Name and Address Information") Consultations

Further to your invitation for public comment, I welcome the opportunity to join other Canadian Information and Privacy Commissioners and Ombudsmen in making submissions regarding the customer name and address information ("CNA") consultations.

As you may be aware, our office was involved in the lawful access consultations that took place in 2002 and 2005. In our submissions of December 10, 2002, and April 21, 2005, we urged the Government of Canada to ensure that any new powers were justifiable, proportionate, and subject to strong oversight. While the lawful access proposal currently under discussion has a narrower focus than the earlier proposals, it is equally important that legislators not needlessly undermine the right to personal privacy, nor underestimate the sensitivity of much of the information involved. In this regard I applaud your widely reported September 13th commitment not to compel Internet Service Providers to provide the state with customer information in the absence of a warrant. However, this raises a critical question – why wouldn't all other individuals, such as telecommunications customers, enjoy equal protection under the law?

In this context, it is vital to recall that the core tenet of privacy is the ability of the individual to control the use and dissemination of their own personal information. We know that CNA information is personal information and that all individual customers have the legal right to insist that, subject to narrowly defined exceptions, their CNA information remain private and confidential. The fact that telephone customers often choose to participate in 411 listing services does not displace any other individual's right to choose privacy over accessibility, and to have that choice respected.

.../2

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
www.ipc.on.ca

To their credit, communications service providers generally strive to comply with their legal duty to protect the privacy of their customers' personal information and to exercise appropriate discretion in considering whether to disclose personal information to third parties, including law enforcement officials. Of course, service providers must also comply with warrants issued by the courts.

Having reviewed all the information provided by the Government of Canada to date, I am not convinced of the need for additional powers. The law currently provides for warrant procedures, expedited tele-warrants, and the special exercise of discretion to disclose personal information by organizations without an individual's consent, for example in exigent circumstances. Public Safety Canada has not provided any information to substantiate the claim that efforts to locate next-of-kin in emergency situations have been significantly or routinely frustrated. Nor has the department made a compelling case for a new power to *unilaterally* compel disclosure in the "early stages" of investigations. In any case, if there are gaps in the law, they ought to be addressed within the context of judicial warrant procedures. Granting law enforcement and intelligence officials the power to issue their own administrative "warrants" represents a substantial departure from the legal and constitutional framework in Canada, which is accompanied by the appropriate checks and balances. Such a departure would require extraordinary justification, and a substantial framework for accountability.

We acknowledge that the safeguards discussed in the consultation materials attempt to frame a discussion regarding transparency and accountability. Nonetheless, it is our strong view that this preliminary list of safeguards is inadequate to redeem an approach to CNA information that derogates from constitutional norms. Administrative "warrant" schemes that may be appropriate in the regulatory context are not appropriate for law enforcement and intelligence purposes.

If, at a later time, a case for additional powers is made out, it is our view that any new *judicial* warrant power should be confined to:

> Clearly defined statutory purposes rather than the expansive language of "duties and functions"; and
>
> Circumstances where the authorities can demonstrate to a judge that the particular information sought is relevant to a specific investigation of an offence or is relevant and necessary to the fulfillment of a specific duty.

It is also our view that any new power must be accompanied by a statutory duty to provide notice to the affected individual(s) within specific timeframes.

Within this context, we believe that there must be detailed, written, record-keeping requirements to provide the necessary accountability and support for the requisite audit and review functions.

.../3

In this regard, we continue to believe that it is critical that Parliament and the public learn of the ongoing and cumulative impact of personal electronic communication surveillance and access powers. We note, for example, that the current wiretap reporting practices of provincial and federal Attorneys General vary considerably despite longstanding reporting requirements mandated under the Criminal Code of Canada. Assessing the impact of surveillance or access powers on the privacy rights and civil liberties of the general population requires much more extensive public reporting. In the absence of a focused harmonizing and coordinating authority, privacy rights and civil liberties will continue to suffer from fragmented and inconsistent protections.

Accordingly, we renew our call for the creation of an independent, arm's-length Surveillance and Access Review Agency (SARA), mandated to supervise access to personal communication information and to report annually to Parliament on the use of surveillance and access powers. The Commissioner of such an agency should be an independent Officer of Parliament nominated by an all-party committee of the House of Commons and appointed by the Governor-in-Council, with sufficient security of tenure to ensure independence and sufficient powers and resources to carry out the mandate of the Office to ensure the desired transparency and accountability. For more information about the functions and duties of SARA, I attach our April 21, 2005 letter to the then Minister of Justice, Irwin Cotler.

Conclusion

Lawful access powers designed for preventative and prosecutorial investigations raise special concerns requiring rigorous oversight and review. These concerns are multiplied in the context of police demands for new powers related to CNA information tied to digital communications. Linking the identity associated with digital devices, as well as IP addresses, to real people presents a number of complexities. Digital identities are often unstable, vulnerable to misuse by third parties, and can be associated with membership in a community rather than simply denote individual use. Risks associated with erroneous linkage by law enforcement and security officials are very significant for individual privacy, reputation and liberty. Due diligence, including that provided by judicial warrant procedures, is necessary to protect the legal rights and interests of all Canadians.

In my view, neither the current law, nor the latest proposals provide for sufficiently robust or dynamic privacy protections. New technologies continue to appear, surveillance and access capacities continue to grow, placing privacy rights increasingly at risk. Governments have a duty to be mindful that, in the absence of adequate safeguards today, the privacy rights of Canadians will be harmed by function creep tomorrow as new tools and new powers are put to new uses. Any proposal to significantly expand surveillance and access powers without providing for a corresponding increase in independent oversight has not and, in my view, cannot be justified. If there are gaps in the law, they ought to be addressed within the context of judicial warrant procedures and supplemented by the establishment of an independent, arm's-length Surveillance and Access Review Agency.

.../4

In closing, I thank you for your recent efforts to involve the public in stakeholder consultations. In order to advance the public debate around these critical issues, I will be posting this letter on our website. If I can be of any further assistance, please do not hesitate to contact my office.

Sincerely yours,

Ann Cavoukian, Ph.D.
Commissioner

Enclosure

Information and Privacy Commissioner/Ontario
Commissaire à l'information et à la protection de la vie privée/Ontario

April 21, 2005

The Honourable Irwin Cotler
Minister of Justice and Attorney General of Canada
House of Commons,
284 Wellington Street
Ottawa, Ontario K1A OA6

Via E-mail/Courier

Dear Minister:

Re: The 2005 "Lawful Access" Consultations

Commissioner Ann Cavoukian has asked me to write you in response to the federal government's 2005 "Lawful Access" proposals. The Ontario Information and Privacy Commissioner's mandate includes commenting on developments that affect the personal privacy of Ontarians. The current proposals clearly do. Accordingly, we welcome the opportunity to join other Canadian Privacy Commissioners and Ombuds Officers in this critical public consultation.

First, please accept our thanks for having your staff and multi-department project team attend at our office. The presentations and subsequent discussions were very helpful. What follows is our response to six power point slide decks and the oral presentation provided on March 7, 2005 (*Combating cyber-crime: the context*, March 2005; *E-mails: Considerations for Criminal Law Policy*, March 2005; *Lawful Access Proposals: Proposals with Respect to Compelling Interception Capability and Access to Subscriber Information*, March 2005; *Lawful Access: Legal Review*, February-March 2005; and *Lawful Access – Amendments to the Competition Act*, March 2005). (More recently, we received and reviewed *Transmission Data: Considerations for Criminal Law Policy*, February 2005.) Should the consultations produce legislative action, we may, of course, provide further comment at that time.

It is apparent that, since Commissioner Cavoukian wrote the Minister of Justice on December 10th, 2002, the "Lawful Access" proposals have evolved. For example, it appears that the government's intention is to limit the surveillance of live communications including in transit e-mail consistent with Part VI of the *Criminal Code of Canada*. This is welcome news. We also applaud the government's decision not to create databanks on subscribers or their day-to-day use of the new technologies. No such databanks should be countenanced. And we encourage you to press forward with the proposal to treat surreptitious video surveillance as a means of "last resort".

.../2

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Télec: 416-325-9195
TTY: 416-325-7539
www.ipc.on.ca

At the same time, we believe that critical elements of the current plans appear to misconceive how Canadians interact with the new communications technologies and significantly underestimate the sensitivity of the personal information involved. The concomitant risks to privacy and other fundamental rights are significant. While we continue to support the vital law enforcement interest in pursuing electronic evidence and intelligence about serious wrongdoing, we also urge the government to ensure that any search and seizure of personal communications be subject to the most rigorous oversight.

Our comments and recommendations relate to three broad themes: 1) the call for a *Privacy and Security Taskforce*; 2) the sensitivity of the personal information involved; and 3) the oversight necessary to counter the risks of broader surveillance and access powers.

1) The Call for a *Privacy and Security Taskforce*

Rapid technological changes are transforming the means, volume, and nature of our *private* communications and *private* activities. We no longer need leave our own homes to shop, study, bank, socialize, or consult. As we participate in this transformation, new information structures arise and a new economy grows. However, in participating, Canadians have not surrendered *their rights* to privacy. Indeed, as reactions to recent information security breaches suggest, Canadians and the companies that service our electronic relationships are becoming increasingly concerned about confidentiality and the protection of personal privacy.

Like the traditional storefront economy, the new web-based economy is dependent on establishing and maintaining trust. Routine government surveillance is as capable of undermining that trust as poor corporate security. Nor is trust enhanced by transforming companies doing online business into virtual agents of the state. And yet, since 2002, federal legislation has been passed that encourages or even requires such entities to engage in surreptitious evidence gathering.

In focusing on intrusive new powers, there is a risk that we endanger proactive innovation. By facilitating surveillance and access, we may even inadvertently make our communications systems more vulnerable to illegal access. Canadians have been leaders in developing new technologies. In our view, Canadians are possessed of untapped ingenuity and enterprise with respect to developing measures to enhance security, safety, and privacy.

Accordingly, we urge the Government of Canada to publicly commit to cooperation with universities, the private sector, non-governmental organizations, and other Canadians in investing in educational, technological, and privacy enhancing preventative measures to combat identity theft and other cyber-facilitated wrongdoing. Privacy and security would both benefit from a coordinated effort to enhance the national and international standards in foundation documents, authentication procedures, encryption technologies, user control, and software design. A *Privacy and Security Taskforce* dedicated to facilitating such work should be struck.

.../3

Legislative reform should not precede such an undertaking. As a founding member of the Privacy Enhancing Technologies Testing and Evaluation Project, our office would be pleased to provide whatever assistance we can.

2) **The Sensitivity of the Personal Information Involved**

Until recently, real-time electronic eavesdropping on private communications has arguably been the most intrusive form of surveillance. Innocent individuals who make or receive a call through a wiretapped telephone line or who enter a "bugged" room are vulnerable to being swept up in a criminal investigation or an intelligence file. A person's intimate relationships and private exchanges may be noted, recorded, and subject to further investigation. In recognizing these serious risks to privacy, Parliament's response has been to insist on both stringent judicial oversight and annual reporting on police use of this highly intrusive form of surveillance.

In contrast, the 2005 "Lawful Access" proposals would allow the state to collect extensive electronic information and intelligence about individuals without comparable safeguards. At the outset of the 21st Century, the everyday use of new digital technologies routinely generates a highly revealing record of personal information as Canadians go about their day to day lives. It is not necessary to "listen in" *live* to electronic communications in order to capture an in depth data-rich composite of our private and personal activities, movements, intentions, relations, and associations. Access to data stored by telecommunication companies, ISP's, banks, other businesses and institutions, and at home can reveal that personal profile at any time of the day or night.

Indeed, the private content of our *live* telephone communications may be dwarfed by the private content in the digital trail or traffic data created every time each of us sends an e-mail, surfs the Internet, uses a bank card or simply carries a cell phone or text messaging device. While not all of this data is currently stored for any great length of time, much of it will be increasingly subject to ready storage and instant analysis as technological capacities increase and technological costs decrease.

Accordingly, it is our view that any state access to the personal information associated with private electronic communications including communication content, traffic data, as well as location data, must be subject to rigorous independent oversight.

3) **The Oversight Necessary to Counter the Risks of Broader Surveillance and Access Powers**

A) The Role of Judicial Authorization and the Threshold for a Warrant

Recently enacted and newly proposed "production" orders allow the state to access corporate held databases. Because "production" orders are directed in whole or part to the capturing of private electronic communication data, they are comparably as intrusive of privacy as old style

.../4

telephone wiretaps. As indicated above, a week's worth of such data may expose the interactions of families, friends, acquaintances, and associates. And because such orders are served on third parties, the people directly impacted may never learn of such violations of their privacy. Alternatively, they may be surprised to discover the consequences of someone's earlier decision to treat them as "guilty by association". Travel plans may be derailed, jobs may be denied, and persons may be detained or deported. Where the information is shared with the law enforcement and national security authorities of other countries, the person may even be subject to extra-legal rendition. While police must not be denied the power to pursue electronic evidence of serious wrongdoing, Canadians' interest in privacy must not be discarded upon a mere suspicion that someone has committed a minor offence.

In our view, it is essential that more stringent conditions precedent be enacted in relation to state access to this information. Production orders in respect of personal electronic communication should be confined to investigations in respect of the list of serious offences in section 183 of the *Criminal Code*. Before issuing such orders, a high court judge ought to be satisfied that:

- there are reasonable and probable grounds to believe that an offence under section 183 of the *Criminal Code* has been or is being committed,
- other less intrusive investigative methods are likely to prove impracticable,
- measures will be taken to safeguard the privacy of the personal information obtained, particularly of non-suspects, and
- the intrusion is otherwise in the best interests of the administration of justice.

The government also proposes to create a new set of powers that police could invoke to require data managers to locate and hold personal information in documents or databanks. The proposals argue that these "preservation" order powers are necessary to support the production order powers discussed above. In our view, any power to issue a "preservation" order, including the proposal that police officers be effectively empowered to "knock on the door" and order data managers to freeze data, should be confined to the same list of serious offences in section 183.

The 2005 proposals would also provide law enforcement with a broad power to contact Internet and telecommunication service providers and compel them to disclose personal "subscriber information", in some cases within 30 minutes of the demand. At a minimum, we urge you to ensure that any such power is confined to clear and defined statutory grounds. Moreover, in addition to requiring that peace officers document their use of this power, they should also be required to provide service providers with explicit written justification for each demand before access to the identifying layers associated with the personal "subscriber information" is granted.

Finally, all those whose personal information is obtained under a surveillance and access regime should be entitled to notification at the appropriate time. And, in accord with recommendations that follow, state use of these powers and access to this personal information should be superintended and reviewed by an independent agency.

.../5

B) The Role of an Independent Surveillance and Access Review Agency

The proposal states that the supervision provided by prior judicial authorization and complaint-driven oversight under the *Charter*, the *Privacy Act*, and the *RCMP Act* provide sufficient safeguards for the protection of our fundamental rights and freedoms. We are of the view that these protections, while critical, are fundamentally insufficient in this context.

The proposed warrant applications will involve complex, highly technical, and sensitive information. Moreover, warrant applications are necessarily held in camera and *ex parte*. Innocent individuals subject to surreptitious invasions of their privacy may never be in a position to file for let alone find redress. Any in depth public scrutiny of such matters is the exception to a general rule of secrecy.

Furthermore, under your proposal, local, provincial, and federal law enforcement agencies would be empowered to use these intrusive powers in pursuit of both domestic and international investigations. The current reporting practices of provincial and federal Attorneys General vary considerably despite longstanding wiretap reporting requirements mandated under the *Criminal Code of Canada*. Without a focused harmonizing and coordinating authority, inconsistent policies and practices are likely to develop among the various jurisdictions. Privacy rights and civil liberties will suffer from fragmented and inconsistent protections

In order to safeguard our fundamental freedoms and human rights, we believe it is critical that Parliament and the public learn of the ongoing and cumulative impact of personal electronic communication surveillance and access.

Accordingly, we call for the creation of an independent, arm's-length *Surveillance and Access Review Agency* (*SARA*) mandated to supervise access to this highly sensitive personal information and report annually to Parliament on the propriety of the operations of the regime. The Commissioner of such an agency should be an independent Officer of Parliament nominated by an all-party committee of the House of Commons and appointed by the Governor-in-Council with sufficient security of tenure to ensure independence and sufficient powers and resources to carry out the mandate of the Office and ensure the desired transparency and accountability.

There is precedent for such an agency. In Switzerland, the federal agency, *le Services des tâches spéciales* oversees all electronic and mail surveillance and access activities at both the federal and canton level. A Canadian *Surveillance and Access Review Agency* (*SARA*) would superintend each intercept, surveillance and production warrant granted in respect of private electronic communications. Like the Swiss model, *SARA* could perform a screening function, ensuring all conditions precedent are fulfilled before an application for a judicial warrant is made. Where all of the conditions were not fulfilled, the omission would have to be rectified before the warrant application could be filed. *SARA* should be organized such that applications to be made on an exigent basis could be dealt with expeditiously.

The *Agency* could also screen all police preservation and subscriber information requests, as well as vet any electronic communications custodian decisions to voluntarily disclose any *personal*

.../6

electronic communication data to the authorities. (Electronic communication custodians would *include* telecommunications, banking, and web-based companies, as well as any institution, organization, or corporation that routinely handles communication data.) Voluntary disclosures would first be transmitted to *SARA* which would then be empowered to determine whether or not they disclosed evidence warranting disclosure to law enforcement. Under exigent circumstances, police would be able to issue a preservation order or make a subscriber information request directly to a communication custodian. However, both the police and the custodian should be required to report to *SARA* immediately thereafter.

Bearing in mind the need to protect the integrity of any ongoing investigations, *SARA* would ensure the appropriate notification of any individuals whose privacy has been impacted by surveillance or production warrants, preservation or subscriber information requests, or voluntary disclosures. Contemporaneously, the authorities would be required to attest to the destruction of personal information in respect of innocent parties. Similarly, authorities who had received information in error or under a faulty application would report to *SARA* and attest to the destruction of the information.

Critically, *SARA*'s role in superintending all warrants, requests, and disclosures would allow it to study and report on all aspects of the operation of a personal electronic communication surveillance and access regime including:

- the number of warrants and requests sought, granted, and delivered in relation to both Canadian and foreign investigations;
- any concerns about the sufficiency of the case for access, the over-breadth of materials disclosed, or the mishandling of personal information by either law enforcement or electronic communication custodians; and
- an analysis of the offences investigated, the patterns and numbers of innocent and suspected individuals targeted, and the outcomes of the investigations.

SARA might also commission studies on the privacy impact of new communications technologies and personal information handling practices. In any case, *SARA* would issue an annual detailed public report directly to Parliament. It would also be required to alert the relevant Attorneys General whenever it had a reasonable basis to believe that law enforcement officials or communication custodians had misapplied the surveillance and access powers so as to warrant discipline, sanction, criminal prosecution, and/or policy changes. And *SARA* would report annually on the government's handling of any such alerts.

Conclusion

In our view, neither the current law, nor the latest proposals provide sufficiently robust or dynamic privacy protections. And as new technologies appear, surveillance and access capacities tend to grow. The government must be mindful that, in the absence of adequate safeguards today, the privacy rights of Canadians may be harmed by function creep tomorrow as

.../7

new tools and new powers are put to new uses. Any proposal to significantly expand surveillance powers without increasing independent oversight has not and, in our view, cannot be justified.

In light of the above-noted concerns, we urge the Government of Canada to both establish a *Privacy and Security Taskforce* and enhance the privacy protections in the "lawful access" proposals. We strongly urge you to ensure that any further changes to the law are subject to full public scrutiny and debate, and a careful and deliberative legislative process. Changes to the laws governing search, seizure, and surveillance must not only provide law enforcement with the tools to counter technologically sophisticated wrongdoing, they must also ensure that privacy rights in Canada enjoy necessary enduring protections. In particular, any new legislation should clearly provide that any personal information associated with private electronic communications data enjoys a strong legal expectation of privacy backed up by rigorous oversight.

In closing, we thank you for your efforts to consult stakeholders across Canada. In furtherance of advancing the public debate about these critical issues, we will be posting this letter on our website at *www.ipc.on.ca*.. For your convenience, I attach a summary of our recommendations. If we can be of any further assistance, please do not hesitate to contact our offices.

Sincerely yours,

Ken Anderson
Assistant Commissioner (Privacy)

cc:

The Honourable Anne McLellan, Deputy Prime Minister and Minister of Public Safety and Emergency Preparedness
The Honourable David Emerson, Minister of Industry
Sheridan Scott, Commissioner of Competition
Jennifer Stoddart, Privacy Commissioner of Canada
Provincial/Territorial Privacy Commissioners and Ombuds Officers
Christopher Blain, Department of Justice

Summary of IPC/O Recommendations in Response to the Federal Government's 2005 "Lawful Access" Consultation:

The Call for a *Privacy and Security Taskforce*

1. The Office of the Ontario Information and Privacy Commissioner urges the Government of Canada to publicly commit to establishing a *Privacy and Security Taskforce*. Such a taskforce would draw on universities, the private sector, non-governmental organizations, and other Canadians. It would be dedicated to facilitating the development of privacy enhancing preventative measures to combat identity theft and other cyber-facilitated wrongdoing. Legislative reform should not precede such an undertaking.

The Sensitivity of the Personal Information Involved

2. Legislation governing the search, seizure, interception, and surveillance of private electronic communications must provide strong legal privacy protections backed up by rigorous oversight.

3. In particular, state access to the personal information associated with private electronic communications, including communication content, traffic data, as well as location data, must be subject to rigorous independent oversight.

The Oversight Necessary to Counter the Risks of Broader Surveillance and Access Powers

The Role of Judicial Authorization and the Threshold for a Warrant

4. Any power to issue a "production" order in respect of personal electronic communication data should be confined to investigations in respect of the list of serious offences in section 183 of the *Criminal Code*. Before issuing such orders, a high court judge ought to be satisfied that:

- there are reasonable and probable grounds to believe that an offence under section 183 of the *Criminal Code* has been or is being committed,
- other less intrusive investigative methods are likely to prove impracticable,
- measures will be taken to safeguard the privacy of the personal information obtained, particularly of non-suspects, and
- the intrusion is otherwise in the best interests of the administration of justice.

5. "Preservation" order powers should be confined to the same list of serious offences.

6. Any law enforcement power to compel Internet and telecommunication service providers to release "subscriber information" should be confined to clear and defined statutory grounds. In addition to requiring that peace officers document their use of this power, they should also be required to provide service providers with explicit written justification for each demand before access to the identifying layers associated with the personal "subscriber information" is granted.

7. All those whose personal information is obtained under a surveillance and access regime should be entitled to notification at the appropriate time.

The Role of an Independent Surveillance and Access Review Agency

8. The Office of the Ontario Information and Privacy Commissioner calls for the creation of an independent, arm's-length *Surveillance and Access Review Agency* (*SARA*) mandated to supervise access to this highly sensitive personal information and report annually to Parliament on the propriety of the operations of the regime. The commissioner(s) of such an agency should be an Officer of Parliament nominated by an all-party committee of the House of Commons and appointed by the Governor-in-Council with sufficient security of tenure to ensure independence and sufficient powers and resources to carry out the mandate of the Office and ensure the desired transparency and accountability.

9. The *Surveillance and Access Review Agency* would superintend each intercept, surveillance, and production warrant granted in respect of private electronic communications. *SARA* could perform a screening function, ensuring all conditions precedent are fulfilled before an application for a judicial warrant is made. Where all of the conditions were not fulfilled, the omission would have to be rectified before the warrant application could be filed. *SARA* should be organized such that applications to be made on an exigent basis could be dealt with expeditiously.

10. The *Agency* could also screen all police preservation and subscriber information requests, as well as vet any electronic communications custodian decisions to voluntarily disclose any *personal electronic communication* data to the authorities. (Electronic communication custodians would *include* telecommunications, banking, and web-based companies, as well as any institution, organization, or corporation that routinely handles communication data.) Voluntary disclosures would first be transmitted to *SARA* which would then be empowered to determine whether or not they disclosed evidence warranting disclosure to law enforcement. Under exigent circumstances, police would be able to issue a preservation order or make a subscriber information request directly to a communication custodian. However, both the police and the custodian should be required to report to *SARA* immediately thereafter.

11. Bearing in mind the need to protect the integrity of any ongoing investigations, *SARA* would ensure the appropriate notification of any individuals whose privacy has been impacted by surveillance or production warrants, preservation or subscriber information requests, or voluntary disclosures. Contemporaneously, the authorities would be required to attest to the destruction of personal information in respect of innocent parties. Similarly, authorities who had received information in error or under a faulty application would report to SARA and attest to the destruction of the information.

12. *SARA* would issue an annual detailed public report directly to Parliament on all aspects of the operation of a personal electronic communication surveillance and access regime including:

- the number of warrants and requests sought, granted, and delivered in relation to both Canadian and foreign investigations;
- any concerns about the sufficiency of the case for access, the over-breadth of materials disclosed, or the mishandling of personal information by either law enforcement or electronic communication custodians; and
- an analysis of the offences investigated, the patterns and numbers of innocent and suspected individuals targeted, and the outcomes of the investigations

13. *SARA* would also be required to alert the relevant Attorneys General whenever it had a reasonable basis to believe that law enforcement officials or electronic communication custodians had misapplied the surveillance and access powers so as to warrant discipline, sanction, criminal prosecution, and/or policy changes. And *SARA* would report annually on the government's handling of any such alerts.

14. *SARA* would also be empowered to commission studies on the privacy impact of new communications technologies and personal information handling practices.

bc civil liberties association
L'Association des libertés civiles de la Colombie-Britannique

fighting for freedom since 1962

6950-13

Customer Name and Address Information Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON, Canada K1A 0P8

October 10, 2007

Dear Consultation Committee:

I am writing on behalf of the British Columbia Civil Liberties Association (BCCLA). Our Association has made previous submissions during the consultation processes on lawful access held in 2002 and 2005. There is no change in our substantive submission on the issue of what is now being re-branded as "customer name and address information" ("CNA information"), previously known as "subscriber information". We remain adamantly opposed to the lowering of the standard for police access to this personal information. It is our submission that the proposal is a significant expansion of police powers that has never been justified and would clearly violate citizens' rights.

There is no demonstrated need for this significant expansion of police powers

Law enforcement agencies have lobbied for years to acquire the ability to demand access to personal information of customers of telecommunication service providers (TSP's). As noted by numerous commentators, a need for the proposed expanded police powers has never been demonstrated.

Rather than evidence that warrantless access to customers' personal information is needed, the current consultation echoes the previous ones in merely citing hypothetical illustrations. The first example cited in the current consultation backgrounder is a non-investigative situation in which the police are unable to compel customers' personal information from a 'non-cooperative' TSP and as a result are unable to locate next-of-kin in emergency situations. The relevance of this example is dependent on a series of curious assumptions, starting with the assumption that it is these kinds of circumstances in which TSP's are exercising their lawful discretion to require a warrant before releasing customers' personal information. We note that public interest and safety disclosures are currently fully provided for in privacy legislation and we are unaware of any evidence that these provisions are not being appropriately used. Further, in addressing the often-alluded-to example of a safety emergency, the police can conduct warrantless searches in cases of exigent circumstances, which include an urgent threat of serious harm to any person or property.

Along with many other organizations, we have frequently called for evidence that shows that current laws are inadequate in the kinds of scenarios cited by proponents of information-on-demand. Half a decade after the first of these consultations, the case has yet to be made.

There is a reasonable expectation of privacy over this personal information

Police spokespersons frequently comment in the media to the effect that the information at issue is no more sensitive than the information found in the phone book. This is false and misleading. The following items are set out in the consultation document to illustrate the scope of the information being sought by police on demand:

- name
- address(es)
- ten-digit telephone numbers (wireline and wireless)
- cell-phone identifiers
- email address(es)
- IP address; and/or
- Identification of the TSP that owns the telephone number or the IP address used by the customer

These "basic identifiers" (as the consultation document refers to them) are a potentially very rich source of data on a given individual. Privacy experts have long maintained that the proponents of lawful access expansion adopt a disingenuously naïve position on the privacy value of these "identifiers". It is an apparent contradiction to say that the information has nugatory privacy value and yet significant value for investigative and other purposes.

The question is what these "basic identifiers" unlock in terms of other information. For example, *McLean's Magazine* did an investigative story in which a reporter was able to access the Privacy Commissioner of Canada's telephone records using a U.S.-based data broker. The "key" piece of information needed to access her telephone logs was her home and cell phone numbers.

The sensitivity of these "basic identifiers" has been purposefully downplayed. This is information that attracts a reasonable expectation of privacy in law.

The proposed "privacy safeguards" do not safeguard privacy

The list of purported "safeguards" is largely unchanged from those proposed in the past. They represent a continued attempt to characterize as "privacy protections" measures that do in fact not protect privacy. Auditing, reporting, and other schemes of oversight are the kinds of things that civil libertarians call for on a regular basis. We just do not confuse them with privacy protections which, it is axiomatic, must be a system of prior authorization, not post-hoc scrutiny.

Not only do these "safeguards" not genuinely protect privacy, the proposal for an elaborate administrative oversight regime exposes a fundamental tension within the proposal writ large. Essentially, an empire of bureaucracy will be called into existence on the seeming justification that applying for warrants is too much paperwork.

In short, if we have the resources for this privacy-diminishing administrative regime, we clearly have the resources for the *Charter*-respecting regime that currently exists.

The consultation process

Having made extensive submissions on this matter on two previous occasions, we are submitting these most recent comments in a very concise format. We are in fact not able to understand the purpose of this current consultation.

We laud the recent comments by the Minister of Public Safety assuring Canadians that the government will not introduce legislation that would require TSP's to provide customers' information to the police without a warrant. However, that assurance having been made, the rationale for this consultation is quite unclear.

We look forward to further clarification that the matter has been settled in accordance with the Minister's clear and direct promise.

Yours truly,

Micheal Vonn
Policy Director
British Columbia Civil Liberties Association

FIPA

BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

October 12, 2007

Customer Name and Address Information Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON, K1A 0P8

Dear Sirs/Mesdames:

Comments on the Customer Name & Address consultation document

The BC Freedom of Information & Privacy Association (FIPA) would like to present its position regarding the Government's Customer Name & Address (CNA) consultation document. FIPA has previously commented on similar proposals, first known as "lawful access" and then "modernization of investigative techniques", and our last submission is attached for your consideration. Our position remains unchanged.

It was with some surprise that we learned of the Government's new consultation on an old proposal. We were initially dismayed that the consultation was to happen behind closed doors, but were pleased when the Minister of Public Safety opened the consultation to the public.

We are also buoyed by the Minister's unequivocal statement that the Government has no intention of expanding police access to personal information without a warrant. However, while the Minister's statements are positive, we remain troubled because the CNA consultation document contradicts the Minister's stated position.

FIPA wishes to echo the broad concerns of other civil liberties and privacy advocates, and draw the Committee's attention to specific elements of our earlier submissions that are relevant to the CNA proposal. Here are our main concerns:

1. The CNA consultation document states, as previous consultation documents have stated, that: "The objectives of this process are to maintain lawful access for law enforcement and national security agencies in the face of new technologies, while preserving and protecting the privacy and other rights and freedoms of all people in Canada."

   The problem is that the proposals go beyond maintaining existing powers in order to cope with new technology. This is not a proposal which merely provides investigative powers in the virtual world that are parallel to those in the real world.

103 - 1093 W. Broadway, Vancouver, BC V6H 1E2
Tel (604) 739-9788 Fax (604) 739-9148 Email: fipa@vcn.bc.ca Web: www.fipa.bc.ca

The CNA proposal would actually *lower* the threshold currently required to obtain Canadians' personal information and expand the areas in which law enforcement agencies may intrude into the lives of individuals.

2. The consultation document provides no concrete evidence to support the claim that new technologies present challenges to investigations. Nor does it provide evidence to suggest that the expanded powers will in any way improve law enforcement agencies' ability to investigate crimes or prevent terrorist activity, though it implies this.

   Furthermore, internet access has been widely available in Canada for over a decade and cell phone service for even longer. These can hardly be considered new technologies that present new challenges.

3. The consultation document attempts to equate the sensitivity of personal information such as a phone number or address with the sensitivity of an IP address. The two are not equivalent. While the IP address can be described, for the purposes of illustration, as an address in the virtual world in the same way that a street address is an address in the physical world, the comparison is quite superficial.

   The important difference between an address in the physical world and an address in the virtual world is not well understood by most people. Whereas an individual's address does not reveal anything about where the individual goes or what they do in their private lives, the IP address has the potential to reveal all these things. For this reason, law enforcement access to IP addresses is a rather invasive proposal.

FIPA would like to thank the Committee and the Minister for the opportunity to participate in this consultation. At the same time, we have participated in several consultations on lawful access and its cousins, and are troubled that the subject continues to re-emerge. We remain opposed to all these proposals and we hope that they will not be resurrected in the future.

Sincerely,

ORIGINAL SIGNED BY

Richard Rosenberg
President, BC Freedom of Information & Privacy Association
Professor Emeritus, Dept. of Computer Science
University of British Columbia

Cc: Hon. Stockwell Day,
Minister of Public Safety

103 - 1093 W. Broadway, Vancouver, BC V6H 1E2
Tel (604) 739-9788 Fax (604) 739-9148 Email: fipa@vcn.bc.ca Web: www.fipa.bc.ca

THE CANADIAN CHAMBER OF COMMERCE
LA CHAMBRE DE COMMERCE DU CANADA

The Voice of Canadian Business
Le porte-parole des entreprises canadiennes

October 12, 2007

Customer Name and Address Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON K1A 0P8

e-mail: cna-consultations@ps-sp.gc.ca

The Canadian Chamber of Commerce appreciates the opportunity to provide the following comments in response to the Customer Name and Address Consultation. The Canadian Chamber is Canada's largest and most representative business association. We speak for 170,000 businesses of all sizes and sectors through our 350 local chambers of commerce and boards of trade located in every province and territory.

The Canadian Chamber's telecommunications service provider (TSP) members have a long history of cooperation with Canada's law-enforcement and national-security agencies (LEAs) and of facilitating lawful access to electronic communications – subject to appropriate legal process and judicial oversight. That being said, the Canadian Chamber agrees that that there is a lack of clarity for TSPs with respect to the provision of customer name and address (CNA) information. The Canadian Chamber would welcome clarification of the scope of CNA and the circumstances and conditions under which TSPs will be compelled to provide this information to LEAs.

TSP subscribers' personal information is subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), as well as the Canadian Radio-television and Telecommunications Commission's (CRTC) *Confidentiality of Customer Information* rules. PIPEDA allows the release of subscribers' personal information without consent only in limited, explicitly itemized circumstances. One such exemption allows disclosure without subscriber consent when an organization is legally compelled to do so under a court order, warrant or where otherwise required by law. Consistent with PIPEDA and CRTC rules, TSPs generally require a warrant or court order before providing LEAs with customer information.

360, rue Albert St.
Suite 420
Ottawa, Ontario
K1R 7X7

613.238.4000
613.238.7643

www.chamber.ca
info@chamber.ca

In taking steps to clarify TSPs obligations to provide CNA information to LEAs, there are limits to a TSP's ability to provide certain CNA information as quickly as may be desired by LEAs. TSPs face constraints upon their ability to provide information which can come as the result of the volume of requests and the CNA information available to them.

The Canadian Chamber notes that Canadian TSPs desire to continue their positive relationships with LEAs. In addition, mandated data retention requirement could impose significant and unwarranted storage and processing costs on Canadian TSPs and their law-abiding customers.

The Canadian Chamber has consistently advocated for the following if lawful access legislation was introduced:

- internationally-recognized standards for lawful access technical requirements;
- a reasonable transition period (i.e. 12 months) from the time any new lawful access legislation comes into force to when TSPs must implement compliant solutions;
- compensation for the costs incurred in:
    - executing warrants/court orders
    - implementing non-standard lawful access capability requirements
    - implementing lawful access capability requirements on an urgent basis, prior to a reasonable transition period (i.e. 12 months)

Once again, the Canadian Chamber of Commerce appreciates the opportunity to provide comments on this very important issue.

Sincerely,

Michael Murphy
Executive Vice-President, Policy

British Columbia Library Association

October 12, 2007

Customer Name and Address Information Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa , ON, Canada K1A 0P8
Email: cna-consultations@ps-sp.gc.ca

To Whom It May Concern:

This letter is a response to Public Safety Canada's Customer Name and Address Information Consultation. The consolation concerns "lawful access" by law enforcement agencies to customer name and address (CNA) information held by telecommunications service providers.

The British Columbia Library Association, established in 1911 and incorporated under the Societies Act in 1948 is a non-profit, independent, voluntary association. Our more than 830 members include librarians, library personnel, library trustees and other interested individuals; corporate, government, school and academic libraries; publishers and library supply companies. BCLA works to keep the library community in BC apprised of important developments regarding issues of concern to library personnel and others.

Before addressing the content of the consultation document, BCLA would like to note its concerns about the consultation process itself. As reported in the media, the consultation document was originally distributed to only a limited set of stakeholders; intentionally or otherwise, privacy advocates and other civil society groups were initially excluded from the consultation. BCLA strongly urges the government to take greater care in the future to ensure that privacy advocates, other civil society groups, and the general public have the opportunity to participate in such consultations.

The consultation document is premised on the claim that "[l]aw enforcement agencies have been experiencing difficulties in consistently obtaining basic CNA information from telecommunications service providers." However, no evidence has been provided to demonstrate the extent of these difficulties. During previous lawful access consultations in 2002 and 2005, the lack of a demonstrated need for proposed lawful access powers was a common complaint among civil society groups. Any expansion of the powers of law enforcement should be based on evidence of a pressing need for reform, not on unsubstantiated assertions by law enforcement or other stakeholders.

The consultation document lists a number of "possible safeguards" on access to CNA information. All of the listed safeguards should be incorporated into any future lawful access programme to ensure accountability and limit the potential for misuse of lawful access powers. In addition, any future lawful access programme should also include the following safeguards:

Suite 150 – 900 Howe Street, Vancouver BC, Canada V6Z 2M4
Tel: (604) 683-5354 Fax (604) 609-0707
office@bcla.bc.ca www.bcla.bc.ca

1. Requests should be specific to individual users, and law enforcement should be required to provide a specific justification for each request. The consultation document proposes that law enforcement should be required to "record ... the duty or function for which a particular request is made," but this would allow law enforcement simply to claim that the requested information is "required for an investigation," without specifying the nature of the investigation or why the information is needed for it. It would also allow law enforcement to request data on a large body of customers (for example, the name and address associated with all phone numbers which have called or been called by a particular individual), even if some or most of those customers were potentially irrelevant to the investigation. Requiring specific justification for each request would help to ensure that lawful access powers are used in a responsible and accountable manner.
2. There should be judicial oversight of all CNA information requests. Requiring law enforcement to obtain a warrant is another important check on lawful access powers, since it requires law enforcement to demonstrate to an independent and impartial judge that there is a genuine need for access to CNA information. Unfortunately, the authors of the consultation document take it for granted that warrantless disclosure is necessary for law enforcement agencies to carry out their duties. No evidence is provided to show that law enforcement officials have difficulty obtaining warrants for CNA information; no consideration is given to alternatives, such as a streamlined judicial oversight process or a lower evidentiary standard for warrants for CNA information. (Note that BCLA does not necessarily support these hypothetical alternatives.)

Last month, Public Safety Minister Stockwell Day told the Ottawa Citizen, "We have not and we will not be proposing legislation to grant police the power to get information from internet companies without a warrant." BCLA is pleased that the government recognizes the vital importance of judicial oversight and expects that this principle will be enshrined in any future lawful access programme.

We appreciate the opportunity to provide input on this important issue and will be following the government's response with the greatest interest.

Sincerely,

Deb Thomas

Suite 150 – 900 Howe Street, Vancouver BC, Canada V6Z 2M4
Tel: (604) 683-5354 Fax (604) 609-0707
office@bcla.bc.ca www.bcla.bc.ca

October 12, 2007

Customer Name and Address Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON, Canada K1A 0P8

RE: Customer Name and Address Information Consultation

The Canadian Wireless Telecommunications Association ("CWTA") is pleased to provide the following comments to Public Safety Canada in response to the discussion paper on Customer Name and Address information ("CNA"). CWTA is the authority on wireless issues, developments and trends in Canada. It represents cellular, PCS, messaging, mobile radio, fixed wireless and mobile satellite carriers as well as companies that develop and produce products and services for the industry.

CWTA has been actively involved in the consultative discussions about lawful access and related issues since 2002 when Justice Canada issued its first consultation paper regarding this matter. Any new lawful access requirements will ultimately affect the Association's carrier and technology members.

CWTA has consistently advocated for standards-based technical requirements, appropriate compensation for Telecommunications Service Provider ("TSP") costs, and a phased-in approach for the implementation of any newly required technical capabilities. It is the consensus view of our members that the previous legislative proposal, Bill C-74: *Modernization of Investigative Techniques Act*, failed to address those needs.

CWTA strongly urges the government to include concrete measures to address the industry's concerns in any new lawful access legislation. From a practical perspective, unless our legitimate concerns are addressed, it will be difficult for the industry to support this important initiative going forward. Any new requirements must be compatible with the standards-based technology that is available to TSPs.

Canada's telecommunications industry has a long history of working cooperatively with law enforcement within Canada's legal framework for lawful access to communications and access to customer information. While cellular/PCS licencees are the only TSPs that have any legal obligation to provide specific lawful access capabilities within their networks, all carriers have some capability and all carriers respond to law enforcement needs on a routine basis. Canadian TSPs generally, and wireless carriers in particular, maintain dedicated security departments whose sole purpose is to respond to law enforcement requests and comply with court orders. These services are provided at considerable cost to the carriers.

T 613 233 4888 F 613 233 2032 www.cwta.ca
1110-130 rue Albert Street Ottawa, ON K1P 5G4

Personal information associated with wireless subscribers is subject to the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") rules under the Privacy Commissioner of Canada as well as the *Confidentiality of Customer Information* rules of the CRTC. PIPEDA allows the release of a subscribers' personal information when legally compelled to do so. Unlike wireline telephone numbers, the CRTC considers that wireless telephone numbers are confidential and it requires carriers to treat them as such. CRTC rules allow the release of subscriber's wireless numbers only when carriers are legally compelled to do so.

In order to comply with their obligations under PIPEDA and CRTC rules to protect their customers' privacy, wireless carriers generally require a warrant or court order before providing law enforcement agencies ("LEAs") with confidential customer information. In cases where exigent circumstances or urgent need can be demonstrated, carriers respond to LEAs as quickly and as diligently as possible.

The wireless industry would prefer to continue to provide confidential customer information only subject to court order or warrant except in exigent circumstances. CWTA does, however, agree with Public Safety Canada's observation that there is a lack of clarity for TSPs with respect to the provision of CNA. CWTA would therefore welcome clarification of the scope of CNA and the circumstances and conditions under which TSPs will be compelled to provide CNA to law enforcement. These details should be explicitly identified and clarified in whatever legislation or regulations are enacted.

As mentioned above, wireless carriers maintain dedicated security departments and incur significant costs in order to cooperate and work with LEAs. It is therefore imperative that LEAs compensate TSPs for law enforcement services. This will become even more important if the volume of CNA requests increases under the proposed "no warrant" regime suggested by this consultation. Costs for TSPs to comply will increase substantially along with the increase in requests.

With respect to the specific CNA information under consideration, much of the information listed in the consultation is already available either publicly or via CRTC tariffed services. A variety of third parties provide "reverse look-up" services for Canadian telephone numbers and many of these are provided free of charge on the public Internet. TELUS' LEADS system provides the registered customer's name and the service address of published telephone numbers. Bell's LSPID service provides LEAs with the name of the TSP associated with a 10 digit telephone number. CWTA is not aware of even a single circumstance when law enforcement has demonstrated an inability to obtain CNA information from the wireless industry.

CWTA notes that the types of "basic identifiers" sought for wireless services go well beyond what virtually anyone would consider basic and are much more onerous than those for TSPs using other technologies. IP addresses and dynamic IP addresses, IMSIs, ESNs, IMEIs, and SIM numbers go well beyond basic "tombstone data" normally associated with CNA. For the sake of fairness, consistency, competitive equity, and technological neutrality, wireless carriers should not be compelled to provide greater levels of information than other TSPs.

If the government does take action to define TSP obligations with respect to CNA, it should clearly recognize the limits of TSPs' ability to respond in a timely manner. Given that certain wireless CNA information has always been considered confidential, systems that can provide quick response for directory assistance have never been developed for wireless services. Wireless carriers work diligently to respond to LEA requests, but face constraints on their ability to provide information. These limitations may be a result of the volume of requests, the details required, or other factors, but it should be recognized in whatever requirements may be imposed that TSPs cannot always respond as quickly as may be desired.

CWTA further notes that wireless carriers do not always have any business reason to collect customer information, and so do not have verified CNA data in their possession in all circumstances. As you will

recall, CWTA addressed this in its comments to the Department of Justice Canada dated December 16, 2002:

> The CWTA strongly opposes the imposition of [a provision of subscriber or service provider information] obligation beyond those situations where a wireless carrier is already collecting this information. Moreover, the CWTA is of the view that service providers should not be liable for the accuracy of customer name and/or address information. In this regard, the CWTA would note that the European Convention refers to subscriber information in that service provider's possession or control.
>
> Generally, wireless carriers collect, validate and maintain customer information to the extent that such information is necessary to successfully provide service and to collect payment. For postpaid services (services for which the customer receives a monthly bill), wireless carriers would typically undertake a credit check to determine a prospective customer's ability to make monthly payments for the services provided. However, this process is geared to validating credit worthiness, not customer name and address. Wireless carriers do not undertake exhaustive validation of the information that is provided by customers and wireless carriers do not warrant that such information is valid or correct, or that it would satisfy the requirements of law enforcement and security agencies. Further, wireless carriers are almost entirely reliant on customer initiated notification with respect to address changes.
>
> Consequently, the CWTA opposes the imposition of any obligation for service providers to collect information that they are not already collecting for their own purposes. Significant service, business and cost issues would arise if wireless carriers were required to collect, validate and maintain accurate customer information for the purposes of lawful access.
>
> First, any such requirement would likely obligate wireless carriers to insist that customers present a minimum degree of official identification at the point of purchase. This would also require that wireless carriers, and the literally thousands of independent distribution agents and outlets they rely on, would be capable of validating such identification. CWTA notes in this regard the concerns raised by the Privacy Commissioner of Canada.
>
> Second, an overwhelming issue arises with respect to on-line purchases of a wireless service since, for these purchases, the entire transaction is conducted over the Internet, not in person. Similarly, customers who opt for on-line billing will be billed on-line and will not have a monthly invoice sent to a physical address. If they chose to move, the carrier will have not means of knowing, apart from the customer taking the initiative to update this information by accessing their on-line account. In the case of purchasing or billing, on-line transactions do not lend themselves to the presentation and validation of the customer's identification. Wireless carriers, and countless other businesses in Canada and abroad, have already made significant investments in on-line purchasing, billing and customer relations capabilities and they rely on this channel as a useful and cost-effective means by which to acquire, bill and interface with their customers.
>
> Third, another problem is created with respect to prepaid wireless services provided by wireless carriers since valid customer information is not required by carriers in order to provide prepaid services. Given that a credit check is not required, and that the customer will never receive a monthly bill, there is no need for the carrier to request the customer's name or address. The entire transaction of activating the customer's account can be conducted over the phone and absent any identification. Although wireless carriers are increasingly requesting customer name and address information for business purposes, this information

is not validated, nor do carriers deny service if the customer does not provide the information.

It should be noted that this situation is not isolated to wireless phones. The verification of a customer's address is only necessary when a service provider must establish a physical connection to the customer. For example; Direct Broadcast Satellite, Multipoint Distribution Service, dial-up Internet Service Providers, and prepaid local and long distance phone card providers are also capable of providing service without knowing the address of the customer.

All of the foregoing remains true today, and CWTA continues to oppose any obligation that would require TSPs to collect customer information beyond what is already collected for business purposes.

Conclusion

The CWTA recognizes that lawful access to communications and the ability to obtain CNA information are important tools for law enforcement. To function properly, however Canada's lawful access regime must recognize the realities of the telecommunications industry:

- TSPs must be compensated for the significant costs incurred responding to the requirements of LEAs.
- Any new technical requirements must be based on international standards, and provide an adequate phase-in period.
- The scope of CNA information and the circumstances under which it would be provided by TSPs to law enforcement should be explicitly identified and clarified in whatever legislation or regulations are enacted.
- CNA requirements should be applied in a technologically and competitively neutral fashion.
- TSPs should not be required to collect customer information beyond what is already collected for business purposes.

CWTA appreciates the opportunity to provide these comments. Given that there are no proposals in this consultation, CWTA requests the opportunity to comment on any changes the government intends to make to the current lawful access regime.

CWTA believes that the importance of this matter warrants full disclosure of the issues involved and encourages the Department to make all comments received through this consultation public. CWTA will be posting these comments on the Association's website.

Sincerely,

Filed electronically

J. David Farnes
Vice President,
Industry and Regulatory Affairs

Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

Philippa Lawson
Director
(613) 562-5800 x2556
plawson@uottawa.ca

6952-13

October 15, 2007

BY EMAIL AND MAIL

Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON
K1A 0P8

Dear Sir/Madam:

Re: Customer Name and Address Consultation

1. The Canadian Internet Policy and Public Interest Clinic ("CIPPIC") is a legal clinic based at the University of Ottawa, Faculty of Law. CIPPIC's mandate includes intervening in legal and policy-making processes on issues arising from the use of new technologies, the outcomes of which have broad public interest implications. Our goal is to ensure that important public interest voices are heard in the policy-making process so that results reflect more than strong vested interests.

2. Public Safety Canada, in collaboration with Industry Canada, has initiated a public consultation on the issue of "updating Canada's lawful access provisions as they relate to law enforcement and national security officials' need to gain access to CNA [Customer Name and Address] information in the course of their duties."[1]

3. The following are CIPPIC's comments in response to the Consultation Paper.

Background

4. The government's Consultation Paper sets out law reform proposals that closely reflect those proposed by the Liberal government two years ago in Bill C-74, the *Modernization of Investigative Techniques Act*, which died with the 38th Parliament when an election was called shortly thereafter. An identical bill was later introduced by Liberal M.P. Marlene Jennings as a private member's bill (Bill C-416), but this bill also died on the order paper when Parliament was prorogued.

[1] See "Customer Name and Address Information Consultation" Document, Online: <http://securitepublique.gc.ca/prg/ns/cna-en.asp>.

5. The proposals to give law enforcement agencies easier access to basic information about telecommunications subscribers have been mooted by the federal government for a number of years. In 2002, the Canadian government announced plans to modernize its criminal law and establish new rules regarding "lawful access" in light of the challenges posed by new technologies to law enforcement. That year, the government consulted with stakeholder groups, including civil society, on a number of ideas including the creation of a national CNA database. Over 300 submissions were received, many from individuals and organizations concerned about the potential impact of the proposals on privacy and civil liberties.

6. In early 2005, government officials initiated targeted, closed consultations with stakeholders (including industry and civil society) on revised proposals, having taken into account the input received in earlier consultations. The revised proposals included "warrantless" access to CNA information.[2]

7. In both sets of consultations, civil society raised serious concerns about the impacts of the proposals on the privacy and civil liberties of individuals, and expressed opposition to proposals for warrantless access to subscriber data. CIPPIC has summarized the consultations and views expressed by civil society in a webpage located at http://www.cippic.ca/projects-cases-lawful-access/. This webpage also includes links to written submissions and other relevant documents.

8. Bill C-74, the *Modernization of Investigative Techniques Act*, was introduced in November 2005. Among other things, the bill included provisions requiring telecommunications service providers to hand over certain subscriber identifying information to law enforcement agencies upon request, without any need for reasonable grounds to suspect criminal activity and without a court order, warrant, or other judicial authorization. The bill did not get past First Reading before an election was called.

9. The current Consultation focuses on essentially the same proposal for warrantless access by law enforcement agencies to customer name and address ("CNA") information from telecommunications service providers.

10. According to the most recent consultation paper, "[t]he objectives of this process are to maintain lawful access for law enforcement and national security agencies in the face of new technologies while preserving and protecting the privacy and other rights and freedoms of all people in Canada," while ensuring "that the solutions adopted do not place an unreasonable burden on the Canadian public."

The Problem

11. The proposals in question are designed to address problems currently being experienced by law enforcement agencies. The Consultation Paper explains the problem as follows:

---

[2] By "warrantless access", we mean the right to demand and obtain such information without a warrant, court order, or other judicial authorization, and without reasonable grounds to suspect criminal activity.

Law enforcement agencies have been experiencing difficulties in consistently obtaining basic CNA information from telecommunications service providers (TSPs). In the absence of explicit legislation, a variety of practices exists among TSPs with respect to the release of basic customer information, e.g., name, address, telephone number, or their Internet equivalents. Some companies provide this information voluntarily, while others require a warrant before providing any information, regardless of its nature or the nature of the situation. 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. This poses a problem in some contexts. For example, law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation. The availability of such building-block information is often the difference between the start and finish of an investigation.

12. The problem thus seems to have two distinct aspects:
    a) locating next of kin in emergency situations, and
    b) gathering CNA information during the early stages of an investigation.

Locating next-of-kin in emergency situations

13. With respect to the former, the appropriate solution is to require that TSPs hand over the necessary information upon request *for the purpose of locating next-of-kin in an emergency situation*; it is not to allow police to demand such information for the much broader purpose of "performing an official duty or function". Especially where fundamental civil liberties are at stake (see below), solutions should be tailored to the problem at hand.

Gathering CNA information in early stages of investigations

14. The second aspect of the problem, as stated in the Consultation Paper, is more troubling. It is not clear whether the problem here involves situations where:
    a) the police *have* reasonable grounds to suspect criminal activity but need to act immediately and don't have time to obtain a warrant;
    b) the police *have* reasonable grounds to suspect criminal activity but simply don't want to go through the process of obtaining a warrant; or
    c) the police lack reasonable grounds to suspect criminal activity and therefore *can't* get a warrant to obtain the information.

15. In the first situation, section 487.11 of the *Criminal Code* allows police to engage in searches without a warrant "if the conditions for obtaining a warrant exist but by reason of exigent circumstances it would be impracticable to obtain a warrant." Presumably, the problem here is that the police can't obtain the information in question without the cooperation of the TSP, and some TSPs are not cooperating. As with the emergency situation described above, this situation can and should be addressed with provisions tailored to the problem in question. Thus, if the problem is that TSPs are refusing to hand over subscriber information regarding someone the police have reasonable grounds to believe is engaging in criminal activity, and if the urgency of the matter justifies proceeding without a warrant, then the proposed law should permit the police to demand production of information where such criteria are met.

In practical terms, the police officer requesting the information from the TSP should be required to communicate the grounds for the request to the TSP, as well as to record it for audit purposes.

16. If police simply want to be relieved of the administrative effort of obtaining warrants for CNA information in cases where they *have* reasonable grounds, we again submit that the proposed solution is too broad. First, it is not clear how the public will benefit by relieving the police of due process requirements in cases that do not involve exigent circumstances. More evidence of how due process requirements regarding CNA information are currently impeding legitimate investigations is needed before mandating disclosure without a warrant requirement. Second, as noted below, CNA information, especially in the digital context, is much more than mere "tombstone" data. It can open the door to a host of detailed information about the individual. We therefore see no reason to apply a lower threshold for access to CNA information than to other information about subscribers.

17. Assuming, however, that there is good reason to relieve police of the warrant requirement for CNA information (as opposed to other information) where they *have* reasonable grounds to suspect criminal activity, then once again, the proposed solution is too broad. Binding requests for CNA information should be limited to those made for the purpose of investigating suspected criminal activity where the requestor has reasonable grounds to believe that a crime is being, has been, or will be committed. Even if third party authorization is not required, "reasonable grounds" can be required and police can be held accountable after the fact. As noted above, the police officer making the request should be required to state the grounds for the request to the TSP, and to record it along with relevant evidence for audit purposes.

18. If, on the other hand, the problem is that the police want to be able to gather CNA information when they have *no* reasonable grounds to suspect criminal activity, we submit that the proposal is unacceptable. Such requests, in our view, constitute "fishing expeditions" and violate fundamental principles of due process. In free and democratic societies, police should not be engaging in proactive investigations without any reasonable grounds to suspect criminal activity. To allow such investigations is to invite abuse. We doubt that it would withstand a *Charter* challenge. Our laws of due process have been carefully crafted so as to balance police powers with civil liberties. Allowing what amount to forced searches without any requirement for reasonable grounds to suspect criminal activity would upset this balance.

Definition of "lawful authority" in subs.7(3)(c.1), PIPEDA

19. Although not stated in the Consultation Paper, we understand that there is another problem underlying the proposal for easier access to CNA information. According to law enforcement agencies and victim rights advocates, some TSPs demand warrants before handing over CNA information because they interpret subs.7(3)(c.1) of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") as requiring such

authorization.[3] PIPEDA contains a number of exceptions to the general rule that organizations must not disclose information about identifiable individuals (including CNA information) without consent. These exceptions include the following:

> *(c)* [where] required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;
>
> (*c*.1) [where] 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;

20. The term "lawful authority" in subs.7(3)(c.1) is not defined in the Act. Apparently, it is being interpreted by some TSPs as requiring authorization in the form of a warrant, court order, or other judicial authorization.[4] Hence, some TSPs consider themselves prohibited from disclosing CNA (and other personal) information to the police unless the request is accompanied by a warrant.

21. It is our understanding that this interpretation was not intended by the drafters of PIPEDA or by Parliament when it passed PIPEDA. Subs.7(3)(c) already provides for disclosures in response to warrants, court orders, etc. Subs.7(3)(c.1) was added in order to preserve the *status quo*, under which organizations were free to disclose personal information to law enforcement agencies even without any warrant or other formal authorization. The term "lawful authority" was meant, we believe, to refer to the institution's authority, not to due process requirements. Although we support those organizations that choose not to disclose other than in response to warrants, it is our understanding that PIPEDA gives the organization discretion to make that choice; it does not prohibit such disclosures.

22. To the extent that the problem underlying these proposals stems from this misinterpretation of subs.7(3)(c.1) of PIPEDA, we submit that the appropriate response is to define "lawful authority" in PIPEDA. It is not to substantially change the law so as to remove the discretion of organizations to demand warrants before handing over their subscribers' identifying information.

---

[3] See Submissions and Testimony of the Canadian Chiefs of Police and the Canadian Resource Centre for Victims of Crime to the House of Commons Standing Committee on Access to Information, Privacy and Ethics in its review of PIPEDA, Meeting No.30, Feb.13, 2007, online: <http://cmte.parl.gc.ca/Content/HOC/committee/391/ethi/evidence/ev2695445/ethiev30-e.htm#Int-1895029>

[4] Hereinafter, we use the term "warrant" to cover all forms of court orders or judicial authorization.

Reasonable expectations of privacy in CNA Information

23. According to the consultation paper, the proposals are designed to assist law enforcement and national security agencies in determining the identity of telecommunications service subscribers, and "would not, in any formulation, include the content of communications or the web sites and individual visited while online." The CNA information in question "could include the following basic identifiers associated with a particular subscriber":
    - name;
    - address(es);
    - ten-digit telephone numbers (wireline and wireless);
    - Cell phone identifiers, e.g., one or more of several unique identifiers associated with a subscriber to a particular telecommunications service (mobile identification number or MIN; electronic serial number or ESN; international mobile equipment or IMEI number; international mobile subscriber identity or IMSI number; subscriber identity module card number of SIM Card Number);
    - e-mail address(es);
    - IP address; and/or,
    - Local Service Provider Identifier, i.e., identification of the TSP that owns the telephone number or IP address used by a specific customer.

24. If this proposal were to go forward, it is essential that the scope of information subject to the new rules be highly constrained (certainly, no broader than in this proposal) and not subject to expansion in future years. This is best done by including the definition in legislation, not ancillary regulations.

25. However, the proposal for warrantless access to CNA information is questionable insofar as it is based on the premise that CNA information attracts a lower expectation of privacy than does other (e.g., message header or content) information associated with individuals. While names and addresses may *generally* attract a lower expectation of privacy than do other types of personal information, that is not necessarily true - especially in the electronic context. Names and addresses can be keys to a host of sensitive personal information such as financial records and health details, much of it available by simple internet searches. As some commentators have noted, allowing unfettered access to CNA information:

> …will bestow upon law enforcement officials a reservoir of personal information from which to fish. These deep basins will allow officials to cast their nets wide, enabling access to personal information that reveals core biographical data…. *typical subscriber information of the sort made available under the proposed … scheme will become the means by which a biographical core of personal information is assembled*.[5]

---

[5] Daphne Gilbert, Ian R. Kerr and Jena McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers," (2007) *Criminal Law Quarterly*, vol. 51(4) 469 at 502-503 [citing, in part: Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004)].

26. Many people use pseudonyms on the Internet in order to engage in anonymous communications without fear of embarrassment or retribution. They have a high expectation of privacy in relation to their Internet identities, and reasonably so. Unmasking their identities without any kind of judicial authorization or requirement for reasonable cause to suspect criminal behaviour is not consistent with the values of a free and democratic society, and may indeed violate the *Canadian Charter of Rights and Freedoms.*[6]

Charter implications

27. Section 8 of the *Canadian Charter of Rights and Freedoms* provides everyone with "the right to be secure against unreasonable search and seizure."[7] According to the Supreme Court of Canada, s.8 protects people, not places or property.[8] The Court has also found that the protection in s.8 is based on "reasonable expectations of privacy"[9], and that everyone has a reasonable expectation of privacy in their "biographical core of information"- i.e., information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[10] Because CNA information (e.g., IP addresses and associated subscriber names) can easily be linked with online activities and communications that expose intimate details of an individual's life, it engages reasonable expectations of privacy, and thus section 8 of the *Charter*.

28. In order for a search to be considered "reasonable" under section 8, courts have found that there must be "reasonable and probable grounds" to suspect that a crime has been committed.[11] Practically speaking, and most often, this means that a search and seizure must be judicially authorized, after the judge has been satisfied that there are reasonable and probable grounds to believe criminal activity has taken place or will take place.[12]

29. Exceptions to this fundamental rule of due process may be permitted under section 1 of the *Charter* if they "can be demonstrably justified in a free and democratic society." The Supreme Court has set out the following test to determine whether a given measure can be so justified:
    - There must be a *pressing and substantial objective*; and
    - The means must be *proportional*; which implies that:
        (i) the means must be *rationally connected* to the objective;
        (ii) there must be *minimal impairment* of rights; and
        (iii) there must be proportionality between the infringement and objective.[13]

30. We question whether the proposal for warrantless access to CNA information would pass *Charter* scrutiny, given the less invasive law reforms that could be implemented to address

---

[6] *Ibid.*
[7] Section 1 of the *Charter,* however, allows for "such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."
[8] *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at para 23, Dickson citing *Katz v. United States*, 389 U.S. 347 (1967).
[9] *Ibid.* at para 24.
[10] *R. v. Plant* [1993] 3 S.C.R. 281 at 293.
[11] *Supra* note 2 at para 43.
[12] *Supra* note 2 at para 28-29.
[13] *R. v. Oakes*, [1986] 1 S.C.R. 103, 24 C.C.C. (3d) 321, 50 C.R. (3d) 1 at paras 69-71.

the problems raised by law enforcement agencies (see above), and the disproportionate impact on individual privacy that warrantless access to CNA information would have, especially in light of the weak oversight and accountability mechanisms currently in place for law enforcement agencies in Canada.

31. Moreover, the internet is a vibrant forum for expression of political dissent and unpopular views, as well as for the sharing of highly personal information, in large part because of the anonymity that it offers to people. In this context, individuals should not be stripped of their anonymity without due process. Otherwise, valuable free speech (as protected by section 2 of the *Charter*) will be chilled.

32. CIPPIC submits that Canadians have a reasonable expectation of privacy in their CNA information, that forced access to that information constitutes a search and seizure, and that such a search therefore requires prior authorization based on reasonable grounds to suspect criminal activity. Allowing for such searches without warrants or other judicial authorization on a "reasonable grounds" basis would, in our submission, violate the *Charter*.

Safeguards

33. The primary safeguard against police abuse of investigative powers is the requirement for prior judicial authorization before a search or other surveillance activity takes place, based on a "reasonable grounds" standard. The proposal in question would do away with precisely that safeguard. For this reason, we object to it.

34. Another critical safeguard is the existence of effective oversight mechanisms to guard against and punish abuse of power. As the Arar Commission's report makes clear, current oversight mechanisms for Canadian national security and law enforcement agencies have proven themselves inadequate in preventing inappropriate sharing of personal information among law enforcement agencies.[14] Without improvements to our current oversight mechanisms, we should not be granting any additional powers to law enforcement agencies.

35. In this respect, we support the Ontario Information and Privacy Commissioner's call for the creation of an independent oversight body to supervise lawful access activities of law enforcement agencies and ensure public accountability, transparency, and scrutiny, and to enhance public confidence, especially if any new "lawful access" powers are granted to law enforcement agencies.[15]

36. The Consultation Paper proposes a number of "possible safeguards", some of which are aimed at oversight. These include:

---

[14] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Public Safety and Emergency Preparedness Canada, 2006). Online: <http://www.ararcommission.ca/eng/AR_English.pdf>

[15] The Ontario Information and Privacy Commissioner proposed such a body in its submission to the Minister of Justice and Attorney General of Canada on the 2005 "Lawful Access" Consultations. See <http://www.ipc.on.ca/index.asp?layid=86&fid1=105>

- requiring regular internal audits by agency heads to ensure that any requests for CNA information are being made in accordance with the protocols and safeguards in place;
- reporting to responsible ministers on the result of any internal audits;
- provision of any audit results to the Privacy Commissioner of Canada, the Security Intelligence Review Committee, or provincial privacy commissioners, as appropriate; or
- provision for the Privacy Commissioner and SIRC to conduct audits related to the release of CNA information.

37. In our submission, internal auditing requirements and discretionary external audits by the Privacy Commissioner of Canada and SIRC are insufficient. Agencies have a strong disincentive to revealing their own errors and weaknesses. Moreover, existing oversight bodies often lack the resources to take on new tasks that they are not mandated to take on. For these reasons, effective oversight should include:
    - a mandatory external audit;
    - mandatory reporting to the Minister and oversight agencies; and
    - a mechanism for public accountability (e.g., reporting to Parliament; publishing of reports).

38. The Consultation Paper suggests a number of other possible safeguards, including:
    - clear limitations on what customer information could be obtained upon request;
    - limiting the number of employees who would have access to CNA;
    - requiring that individuals with access be designated by senior officials within their organizations; limiting requests to those made for the purpose of performing an official duty or function;
    - requiring that requests be made in writing, except in exceptional circumstances;
    - requiring that designated officials provide associated information with their request, e.g., identification of a specific date and time for a request relating to an IP address;
    - requiring designated officials to record their status as such when making a request, as well as the duty or function for which a particular request is made;
    - limiting the use of any information obtained to the agency that obtained it for the purpose for which the information was obtained, or for a use consistent with that purpose, unless permission is granted by the individual to whom it relates.

39. In order for auditing and accountability mechanisms to be effective, officers accessing CNA information should be required to keep detailed records including the purpose for demanding access – not just "the duty or function for which a particular request is made".

40. With respect to safeguards against misuse of information gathered, we submit that there should be strict limits on disclosure as well as use of the information gathered. Moreover, there should be stiff penalties for opportunistic use, or misuse of information accessed through the new power.

41. Even with all these safeguards, however, the proposal to permit warrantless access to CNA information remains in our view fundamentally flawed due to its over-broad nature – i.e., permitting access without warrant or reasonable grounds as long as it is "for the purpose of

performing an official duty or function". If law enforcement agencies are to be granted wider powers to access this information, a key safeguard is to limit the purposes for which they can demand access much more narrowly than this.

Conclusion

42. Information identifying telecommunications subscribers can be highly sensitive given the electronic trail of publicly available and otherwise accessible data that individuals now leave about themselves on the internet and other digital devices as they go about their daily lives. For this reason, we submit that CNA information raises a "reasonable expectation of privacy" on which a *Charter* challenge to laws permitting warrantless access could be based.

43. Moreover, we remain skeptical about the need for these potentially intrusive and far-reaching measures. It is not clear that greater access by law enforcement to electronic communications will, in fact, increase the security of Canadians; and it has not been demonstrated that no other, less privacy-intrusive, measure would suffice to achieve the same purpose of enhanced security. In particular, the permitted purposes for demanding CNA information are far broader than required to solve specific problems such as gaining access to next-of-kin information in emergency situations, or acting on tips quickly in exigent circumstances.

44. Finally, the safeguards proposed are insufficient, in our view, to protect individuals from over-reaching and abusive exercise of police powers. In particular, there should be no expansion of police investigatory powers without a corresponding increase in independent oversight.

Sincerely,

Philippa Lawson
Director, CIPPIC

Jocelyn Cleary
Student-at-law, CIPPIC

Vancouver Community Network

- the regional FreeNet

October 18, 2007

By fax and email: 613 954 5186 and cna-consultations@ps-sp.gc.ca

Customer Name and Address Information Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON, Canada K1A 0P8

Dear Consultation Committee:

Re: Lawful Access Legislation – Public Consultation

We write in relation to the consultation that has been undertaken by your ministry regarding possible new legislation that would allow the police to obtain subscriber information from internet service providers (ISPs) without court authorization.

The Vancouver Community Network is a non-profit ISP dedicated to making the information highway accessible to everyone. We have approximately 10,000 individual and 1000 group users, mostly in the Lower Mainland of British Columbia. We provide our users with free dial-up internet access, email accounts, website space, email lists, and other services.

We are totally opposed to any legislation that would force our staff members and volunteers to disclose any personal information about one of our users, unless required to do so by a court order based on probable cause to believe that the user has committed a serious crime. We believe that those circumstances are adequately addressed by the existing provisions of the Criminal Code, and that no new legislation is needed for the investigation of internet-related crime.

In our view, any legislation that purports to allow such access would violate the Charter of Rights and Freedoms. In 2001, our membership resolved at our annual general meeting that no information regarding our users or their online activities would be disclosed without a valid court order. We regard that as a promise by our society to our users that their privacy rights will be respected.

411 Dunsmuir Street
ph. 604 257 3804
www2.vcn.bc.ca
registered charity

Vancouver BC V6B 1X4
fax: 604 257 3808

BN 14101 7152 RR0001

Vancouver Community Network

- the regional FreeNet

We fully endorse the submissions of the BC Civil Liberties Association dated October 10, 2007 and the Canadian Internet Policy and Public Interest Clinic dated October 15, 2007.

We also call your attention to the concerns expressed by the Privacy Commissioner for British Columbia, in his April 8, 2005 letter to Ministers McLellan, Cotler, and Emerson, when a similar proposal was under consideration:

> • *The proposed new power for law enforcement officials to compel disclosure of subscriber information without cause and without prior judicial authorization is of significant concern. I remain concerned about whether such a new power is truly necessary. Certainly, law enforcement agencies should have the power to compel such information only where the person making the demand has reason to believe the information is necessary for a law enforcement investigation respecting a criminal offence.*

We are heartened by Minister Day's public statements that this consultation was initiated without his knowledge or approval, and that the government has no intention of introducing legislation that would permit access to subscriber information without court authorization.

Should any such legislation be proposed or introduced in the future, despite the Minister's commitment to the contrary, we will address it more fully at that time.

Yours truly

James Sayre
President – Board of Directors

xc: Hon. Stockwell Day, Minister of Public Safety

411 Dunsmuir Street
ph. 604 257 3804
www2.vcn.bc.ca
registered charity

Vancouver BC V6B 1X4
fax: 604 257 3808

BN 14101 7152 RR0001

PUBLIC INTEREST ADVOCACY CENTRE
LE CENTRE POUR LA DEFENSE DE L'INTERET PUBLIC
ONE Nicholas Street, Suite 1204, Ottawa, Ontario, Canada K1N 7B7
Tel: (613) 562-4002. Fax: (613) 562-0007. e-mail: piac@web.net. http://www.piac.ca

October 18, 2007

BY E-MAIL ONLY

Customer Name and Address Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON
K1A 0P8

Dear Madam or Sir:

I am writing you on behalf of the Public Interest Advocacy Centre (PIAC) to comment on the "Customer Name and Address Information Consultation" document.[1] To date there have been three such consultations (2002, 2005 and now 2007) by successive governments regarding what also has become known as "Lawful Access".

PIAC is concerned that the Consultation document is short and undetailed in comparison to past materials supplied (sometimes in confidence) regarding what appears to be an identical initiative. Indeed, the Consultation document is so short as to be misleading to the uninitiated. The only real detail provided is two potential justifications for the entire regime – emergency notification and investigative "bootstrapping".

Regarding these two justifications for the warrantless collection and use of "customer name and address information", generally we endorse the criticisms of and questions raised by the response to this consultation made by the Canadian Internet Policy and Public Interest Clinic (CIPPIC).

Regarding emergency situations, we note in addition that PIPEDA already provides an exception for use and disclosure of personal information in a situation that is life-threatening or likely to result in serious bodily harm to an individual, without consent. Although we appreciate that some telecommunications companies may believe they require a warrant for even this sort of access, it is in fact permitted to be used to respond to the emergency by the holder of the information (see PIPEDA, s. 7(2)(b)) or may indeed be disclosed to law enforcement or others in an individual emergency (see PIPEDA, s. 7(3)(e)). The only complication is that the holder of the information that is disclosed must immediately notify, in writing, the subject of the personal information about the disclosure. However, if an emergency is the real purpose for the request, authorities should not take issue with notification to the individual. To the extent that telecommunications providers are reticent about disclosure of personal information in a true emergency situation, it would seem a simple matter of education about the PIPEDA exception.

---

1 "Customer Name and Address Information Consultation" Document, Online: http://securitepublique.gc.ca/prg/ns/cna-en.asp

Warrantless investigation, however, appears to be the larger goal of this consultation. Nothing appears to have changed from the previous consultations: PIAC assumes that what was presented to the few stakeholders who were invited to the consultations mentioned in the Consultation document (we were not) was that the standard for access will be a non-judicial one (where police or other "authorized persons" simply demand the information from telecommunications service providers due to "suspicion" that a subject (or group of subjects) is somehow involved in an undefined or somewhat defined list of "offences"). If we are mistaken in this assumption, we assume that at the least, if any judicial oversight is indeed required, that it will be on less than a "reasonable to believe" standard (the standard for most present wiretap authorizations – although there is also a "reasonable to suspect" standard for certain offences). This is implied by the wording of the Consultation document that reads in salient part:

> For example, law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation. The availability of such building-block information is often the difference between the start and finish of an investigation. [Emphasis added.]

Assuming there is a framework being contemplated that is roughly what has been proposed the last two times, we refer you to PIAC's 2002 comments on "Lawful Access",[2] much of which address the warrantless standard and the civil liberties protected by the *Canadian Charter of Rights and Freedoms* in relation to privacy and search and seizure. It appears the same flaws, from PIAC's point of view, exist in this initiative, with the exception that none have been explicitly addressed in this consultation – which begs the question whether it is deliberately or just negligently obfuscatory.

PIAC further views the CNA information sought to be collected as clearly personal information, either under legal interpretations of various privacy commissioners and courts, or the opinion of the public.[3] Therefore the Minister's statements to the press that: "We have not and we will not be proposing legislation to grant police the power to get information from internet companies without a warrant. That's never been a proposal," and "It may make some investigations more difficult, but our expectation is rights to our privacy are such that we do not plan, nor will we have in place, something that would allow the police to get that information"[4] should not be based on a semantic game if it is an attempt to define CNA as something other than "information" or to suggest it is not private in this context.

Should the government wish to troll through online personal information without judicial oversight, or under a greatly reduced standard of judicial oversight, it should at the least be subject to serious public oversight (by Parliament and the general public), there should be severe penalties for misuse of the information and its collection and use should be restricted to only highly serious and defined offences.

Yours truly,

Original signed

John Lawford
Counsel

---

2 See Public Interest Advocacy Centre, Comments on the Federal Government's "Lawful Access" Consultation Document (December 16, 2002). Online: http://www.piac.ca/files/piac_dec16_02.pdf

3 See PIAC, "Consumer Privacy and State Security: Losing Our Balance" (November 2004) at p. 29, where it is noted that 86% of Canadians in a POLLARA poll indicated they expect government to get a warrant to read their e-mail or monitor their web-surfing habits. Online: http://www.piac.ca/files/statesecurity.pdf

4 See CBC News Online, "Day firm on police warrants for access to internet user data" Online: http://www.cbc.ca/canada/story/2007/09/14/tech-privacy-warrant.html

OFFICE OF THE PRESIDENT
CABINET DU PRÉSIDENT

October 18, 2007

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security Branch
Public Safety Canada
269 Laurier Avenue West
Ottawa, ON K1A 0P8

Dear Ms. Clairmont:

Re: Customer Name and Address Information Consultation

I write in response to your letter dated September 11, 2007, seeking our comments on Public Safety Canada's Customer Name and Address (CNA) Information Consultation Document. This letter summarizes the Canadian Bar Association's (CBA) concerns about proposals pertaining to law enforcement and national security agencies' access to CNA information held by telecommunications service providers (TSPs). Thank you for the opportunity to contribute our views on this important subject.

The CBA is a national professional organization representing over 37,000 lawyers, notaries, law students and teachers from every part of Canada. The CBA's mandate includes seeking improvements in the law and the administration of justice.

Fundamental Principles

In previous consultations on what have been referred to as "lawful access" proposals in 2002 and 2005, the CBA emphasized several fundamental principles. We stressed that all initiatives must be constitutionally valid and reflect fundamental values of Canada's *Charter of Rights and Freedoms*. As a prerequisite to any new investigative powers, we noted that the need for those new powers must be clearly demonstrated and that the measures proposed be carefully tailored to provide the maximum respect for individual rights. We have previously articulated the fundamental importance of the balancing process required as follows:

500 - 865 Carling, Ottawa, Ontario Canada K1S 5S8
Tel/Tél. : (613) 237-2925 Toll free/Sans frais : 1-800-267-8860 Fax/Télécop. : (613) 237-0185
Home Page/Page d'accueil : www.cba.org E-Mail/Courriel : info@cba.org

> *Living in a democracy requires that the state should not interfere with, or restrict the rights, liberty or security of individuals without a demonstrated need. Where there is compelling evidence of such a need, the law or other action of the state should be tailored so that the restriction on, or interference with individual rights is no greater than absolutely necessary to accomplish the objective of the law or state action.*[1]

We repeat that the twin principles of demonstrated necessity and minimal intrusion must form the foundation of any proposals to advance or extend search and seizure powers. This foundation also provides the essential context in which the constitutional validity and efficacy of new measures must be assessed.

The CBA has also previously expressed strong concerns about the potential of various lawful access proposals to profoundly impact the privacy of individual Canadians. We have particularly noted, amongst our other concerns, the potential to destroy solicitor client privilege by violating communications between lawyers and clients.[2]

While we appreciate that access to CNA information has been the subject of previous consultation, the rapid evolution of technology and investigative practice requires careful consideration of the context in which these current proposals are made. In our view, the present context is not described in sufficient detail to permit definitive conclusions about these proposals. However, we believe that this consultation provides an opportunity to articulate a principled framework in which these issues can properly be considered.

Explicit Legal Authority

As noted in the consultation document, a wide variety of practices have developed regarding the release of CNA information to law enforcement authorities. The CBA welcomes recognition of the need for explicit legal authority for the mandatory release of this personal information.

The inconsistent practices of Canadian organizations in general and TSPs in particular, as mentioned in the consultation document, are a direct result of the challenges many organizations have in applying the *Personal Information and Electronic Documents Act* (PIPEDA), specifically section 7(3). PIPEDA provides a regime that governs the collection, use and disclosure of personal information by the private sector, generally requiring knowledge and consent of the individual to whom the personal information pertains. However, section 7(3) also provides for specific limited circumstances where personal information may be collected, used and disclosed without an individual's consent. Relevant to this consultation are section 7(3)(c) regarding warrants and court orders, section 7(3)(c.1) where a request is made by a government institution that has identified its lawful authority, and section 7(3)(i) where the disclosure is "required by law".

The circumstances when a warrant or court order is presented or when disclosure is required by law elicit little confusion. However, there has been significant uncertainty and confusion as to exactly what "lawful authority" includes in relation to requests from law enforcement agencies (LEAs). A detailed analysis of "lawful authority" as intended in section 7(3)(c.1) is beyond the

---

1 Canadian Bar Association, *Submission on Lawful Access* (Ottawa: CBA, 2005) at 1.

2 Canadian Bar Association, Letter from then CBA President B. Tabor to then Ministers of Justice, Public Safety and Industry (Ottawa: CBA, 5 July 2006).

parameters of this consultation. However, it is relevant to note that some LEAs point to this section of PIPEDA as actually constituting their "lawful authority" to obtain the requested information. Certain LEAs have even formulated a "letter of authority" to request CNA information, referring to PIPEDA as their lawful authority.

In fact, section 7(3)(c.1) cannot constitute lawful authority to obtain the requested information. Rather PIPEDA establishes a discretionary regime pursuant to which organizations ***may*** disclose personal information when the relevant requirements of the section in question have been met.

The effect of the amendments proposed in the consultation document would be to remove uncertainty for certain private sector organizations (i.e. TSPs) as to any discretion to disclose the CNA information specified in the consultation document: according to the proposals, they would be "required by law" to disclose the specified information. However, while the consultation document clarifies the nature of an order that would give rise to an obligation to disclose, we note that private sector organizations would continue to have discretionary ability to disclose certain information pursuant to applicable privacy legislation such as PIPEDA.

Prior Judicial Authorization and Reasonable Expectations of Privacy

The consultation document proposes an administrative scheme where a designated officer could demand disclosure of CNA information. Several possible safeguards are suggested in the consultation document, many that appear to respond to some of the issues raised in earlier consultations.[3] We have two principal concerns regarding the model proposed in the consultation document.

First, the disclosure of the stipulated information upon demand appears to be at least partly based on the idea that PIPEDA would not restrict disclosure of certain material because it is already in the public domain through sources such as telephone directories. In fact, PIPEDA does not distinguish between sensitive and non-sensitive information in this context. PIPEDA does permit the disclosure of personal information that is both publicly available ***and*** specified by the regulations. However, most of the information listed in the consultation document is not actually publicly available and is also not specified by the regulations. Still, as noted, disclosures in such contexts fall under a discretionary responsibility and the other PIPEDA provisions would continue to apply to any discretionary disclosure.

Second, the scope of the information listed in the consultation document is much too broad, and extends beyond what might be appropriately regarded as "basic information". Responses to previous consultations on this topic also expressed concern about the scope of proposed lists.[4]

Concerns about the scope and nature of such information must be measured against the constitutional concept of a reasonable expectation of privacy. This concept defines the threshold at which prior judicial authorization for a search will be required.[5] However, it is sometimes difficult to determine precisely where that threshold will fall. The Supreme Court of Canada has

---

3 See for example the response of the Federal Privacy Commissioner to a similar proposal in 2005, "Response to the Government of Canada's "Lawful Access Consultations", available online at http://www.privcom.gc.ca/information/pub/sub_la_050505_e.asp

4 *Ibid.*

5 See for example, *Canada* v. *Southam Inc.*, [1984] 2 S.C.R. 145.

noted that the determination of where a reasonable expectation of privacy will be found is a contextual exercise, requiring a careful balance between the rights of the individual and the legitimate interests of society in effective law enforcement.[6] As technology and investigative practices evolve, previously constitutional activities conducted without warrant may require a warrant. The extent to which changes in technology and practice enable the discovery of "core biographical information" or reveal "intimate details regarding lifestyle" may necessitate prior judicial authorization.[7] Further, the current technological capability to combine various sources of information to reveal additional details about individuals is a significant factor that may favour prior judicial authorization.[8] The CBA believes that a continuing review of any administrative model would be imperative to ensure that changes in technology and practice do not result in a process that violates the *Charter*.[9]

Administratively authorized search procedures, as opposed to court ordered procedures, have been particularly susceptible to abuse. In the United States, a recent review of "National Security Letters" issued pursuant to the *Patriot Act* revealed significant irregularities and abuse in the program.[10] The Office of the Inspector General documented that the use of National Security Letters increased exponentially after that power was expanded in the *Patriot Act*.[11] Difficulties and discrepancies in internal record keeping practices and controls complicated the task of compiling accurate statistics.[12] The American experience should serve as a warning for Canada in relation to administrative programs, and illustrates that significant problems can arise even when a program includes internal restrictions and safeguards.

On a practical note, careful consideration must be given to the impact of increased internal procedures and protocols on the ultimate speed and efficiency suggested as advantages of the administrative model. One result of the appropriate proliferation of internal protocols and safeguards may be to narrow any difference in the time involved between the administrative and judicial authorization process. If this gap is significantly narrowed, diminished practical benefits of the administrative approach must be assessed against the shortcomings and difficulties of that approach noted above. It is important to consider that internal safeguards cannot replicate certain benefits of prior judicial authorization, such as those associated with maintaining public confidence in our laws. Careful consideration must also be given to existing mechanisms contained in the *Criminal Code* that either enable searches for certain information at lower thresholds, or through the use of an expedited process.

---

6 *R. v. Tessling* 2004 S.C.C. 67 at paras. 17-18. See also *R. v. Plant,* [1993] 3 S.C.R. 281 at 293.

7 *Tessling, ibid.,* at paras. 59-62.

8 For example, the impact of new technology on the ability to combine such sources, together with the resulting loss of privacy is described in the context of "data mining" in Renee Pomerance, "*Redefining Privacy in the Face of New Technologies: Data Mining and the Threat to the "Inviolate Personality"* (2006) 9 Can. Crim. L. Rev. 273.

9 We appreciate that Public Safety Minister Stockwell Day has stressed that personal information requires the ongoing protection of judicial authorization.

10 *A Review of the Federal Bureau of Investigation's Use of National Security Letters",* March 2007, United States Department of Justice, Office of the Inspector General, Executive Summary at 34-50. Available online at http://www.usdoj.gov/oig/special/s0703b/final.pdf

11 *Ibid.,* at 17.

12 *Ibid.* at 17-19.

In our responses to the last two consultation documents on lawful access in 2002 and 2005 and elsewhere, the CBA suggested that a comprehensive approach to search and seizure powers in the *Criminal Code* is needed. Such an approach should encompass all forms of search and seizure in a dedicated part of the Code, including intercepts, CNA information, tracking warrants, general warrants and other types of search and seizure.

Finally, the consultation document suggests that information could be obtained for purposes of notification of next of kin or other similar circumstances. However, it would be a relatively uncomplicated matter to deal with such situations. For example, TSPs might notify individuals involved that the authorities have information to provide to them, or specific legislation could be passed to directed TSPs to provide CNA information in that context without prior judicial authorization. However, that unique context is significantly different than an investigation of a *Criminal Code* offence.

Role of the Police, CSIS and the Competition Bureau

The CBA is particularly concerned with the suggestion that the proposed powers should be granted concurrently to the police, CSIS and the Competition Bureau. The uses to which information may be put in the context of investigations by the Competition Bureau or CSIS differ significantly from that of LEAs under the *Criminal Code*.

In our submissions to the Air India Inquiry,[13] the CBA pointed out that information gathered for intelligence purposes is inherently different than information gathered for law enforcement purposes. Information for intelligence purposes is gathered without the expectation that it will ultimately be led as evidence in a court of law. The procedures for gathering, storing, recording and disclosing security information is completely different from that engaged in by police officers in respect to evidence under the *Criminal Code*. Generally, the actions of intelligence officers will never be subject to judicial review. Accordingly the requirement for prior judicial authorization is more, not less, pressing in the case of CSIS or any other agency involved in information gathering for intelligence purposes. As has unfortunately been seen in the Arar Inquiry,[14] intelligence information can be used to have devastating effect on a person's life, without any judicial intervention or review.

Likewise the nature of the *Competition Act* and the investigations conducted by the Competition Bureau under that Act are quite different from the type of investigation carried on by the police. In the context of the *Competition Act*, it is anticipated that voluminous documentation would be an inherent part of the process and that the breaches of law will be aimed primarily at unlawful financial advantage as opposed to threat of physical harm. Realistically, the Competition Bureau is unlikely to require CNA information on an urgent basis such that the absence of prior judicial authorization would be justified.

Conclusion

The CBA appreciates the opportunity to participate in ongoing consultations regarding lawful access and access to CNA information. We have stressed that the determination of constitutional norms in this regard is a context sensitive exercise. Any expansion of the search powers in the

---

13 Canadian Bar Association, *Submission to the Air India Inquiry* (Ottawa: CBA, 2007).

14 Canadian Bar Association, *Submission to the Arar Inquiry* (Ottawa: CBA, 2005).

Criminal Code or other legislation should not occur without a clear and demonstrable foundation. We welcome the opportunity to participate in further discussions once that context has been fully articulated, particularly in relation to present technical and practical capabilities.

We have noted several difficulties with an administrative search regime. The constitutional status of such a regime may be undermined by technological advances, changes in practice or the ability to combine or aggregate data from several sources. Further, there are inherent difficulties with an administrative approach such that it may be that in the long run a system based on prior judicial authorization provides the more constitutionally stable and effective approach. Finally, to the extent that the consultation document proposes a "one size fits all" approach for the *Criminal Code,* the *Competition Act*, and CSIS, we express our concern, and point to the very distinct roles of these statutes and agencies and the contexts in which they generally function. A proper approach must recognize those significant differences.
The issue of costs of complying with either a court order or an administrative order is a complex and contentious one. It is difficult to compare costs of an administrative scheme with one that relies on court orders, given factors such as indirect cost implications to the court system or direct cost implications to the law enforcement agency involved. The current proposals may also have cost implications for TSPs and other third parties. This has been the subject of other consultations, and is a complicated public policy issue. It is also the subject of continuing litigation.[15] We welcome the opportunity to comment during further consultations on this important related issue.

We note too that the issue of extraterritorial application of Canadian laws must be considered as the proposals in the consultation document may indirectly impact organizations or citizens from other jurisdictions. Again, this is a significant and complex issue in an increasingly globalized economy that involves, for example, many internet service providers and offshore data storage.

The CBA believes that the quality of any public consultation process is significantly enhanced by the level of detail provided in the consultation documents. To the extent possible it would be helpful to have concepts presented in as much detail as possible, including examples of draft language for the proposals in question.

We look forward to continuing dialogue on these important issues, and thank you again for the opportunity to participate in this consultation.

Yours very truly,

(original signed by Bernard Amyot)

Bernard Amyot

---

15 See for example *R. v. Tele – Mobile*, tentatively scheduled to be argued in the Supreme Court of Canada in December of this year.

povnet SOCIETY

#300-1140 W Pender Street
Vancouver, BC V6E 4G1
tel: 604-876-8638;
fax: 604-685-7611
info@povnet.org
http://www.povnet.org

October 18, 2007

By mail and fax: 613-954-5186

Customer Name and Address Information Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON, Canada K1A 0P8

To Whom It May Concern:

Re: Lawful Access Legislation – Public Consultation

PovNet is a non-profit society which seeks to help Canadians alleviate poverty by providing online legal information on its public website (www.povnet.org), and by sponsoring confidential email lists and online training for advocates.

Many thousands of people visit our website to find out about many legal issues that affect poor and otherwise disadvantaged people. Many of these issues are very sensitive and personal for the person involved – including mental illnesses, sexual abuse, AIDS and other illnesses, and difficult family problems.

Our email lists provide a confidential means for community advocates, legal aid staff, and others to exchange information and advice about how best to help people facing such difficult problems. We therefore require all those who participate in the list to promise that they won't disclose any of those communications with anyone who is not a member of the list. In short, the lists are used to discuss confidential legal matters.

PovNet is not an internet service provider itself. Our website and email lists are hosted by the Vancouver Community Network (VCN), a non-profit charitable society that was founded to help make the information highway accessible to everyone. As VCN's own

submission explains, its members have resolved not to disclose personal information about its users under any circumstances, unless required to do so by a court order based on probable cause to believe that the user has committed a serious crime. We rely on VCN's promise that it will protect the privacy of PovNet's visitors and email list members.

In our view, the existing provisions of the Criminal Code provide an adequate and appropriate procedure for the police to investigate internet-related crime. We oppose any legislation that would require VCN or other ISPs to turn over personal information about their users without a court order, and we believe that any such law would violate the Charter rights of our visitors and members.

We were heartened by Minister Stockwell Day's statements to the media that this consultation was initiated without his knowledge or approval, and that the government has no intention of introducing legislation that would permit access to subscriber information without court authorization.

Should any such legislation be proposed or introduced in the future, despite the Minister's commitment to the contrary, we will address it more fully at that time.

Yours truly

Penny Goldsmith, Executive Co-ordinator
PovNet

cc: Hon. Stockwell Day, Minister of Public Safety

Name/Organization	Phone Number	Incoming Correspondence/Timing	Outgoing Correspondence/Timing
Signy Arnason/Cybertip	(204) 945-1861	-emailed Amanda (Sept. 13)	-Letter sent (Sept. 10) -Amanda left a message (Sept. 12) -Yacine left a message (Sept. 25) -Yacine left a message (Oct. 2) -Yacine left a message asking about next steps (Oct. 9) -Amanda emailed Cybertip to ask about consultations (Oct. 16)
Avner Levin/Ryerson University	(416) 979-5000 x 7690	-emailed Amanda (Sept. 18)	-Letter sent (Sept. 10) -Amanda called (wk of Sept. 10) -Amanda wrote email (Sept. 18) -Yacine left a message (Sept. 25) -Yacine spoke to him (Oct. 2)
Raymond D'Aoust/Office of the Privacy Commissioner of Canda	Will call us back Oct. 1		-Letter sent (Sept. 10) -Amanda called (Sept. 11) -Amanda talked to them (Oct. 2)
Gaylene Scholenberg/Canadian Bar Association	(613) 237-2925 x 139	-Gaylene called Yacine back and said she would provide written comments (Oct. 9)	-Letter sent (Sept. 10) NOTE: addressed to Bernard Amyot -Amanda called (Sept. 12) -Yacine left a message (Sept. 25) -Yacine called (Oct. 3) -Yacine called and left a message (Oct. 9)
Michael Mostyn/B'nai Brith	(613) 447-2494 (cell)		-Letter sent (Sept. 10) -Yacine left a message (Sept. 26) -Yacine left a message (Oct. 3) -Yacine left a message inquiring re: next steps (Oct. 9)
Clayton Pecknold and Pierre-Paul Pichette/CACP	(250) 544-4230		-Letter sent (Sept. 10) -Jamie and Clayton Pecknold spoke by telephone (wk of Sept. 10) -Jamie and Pierre-Paul Pichette spoke by telephone (wk of Sept. 10) -Jamie left a message (Sept. 25) -Jamie spoke with Clayton by telephone and discussed the nature of CACP consultation submission (Oct. 4) -Amanda called Clayton Pecknold and he said that he would provide a

			written submission (Oct. 16)
Bill Munson/ITAC	(905) 602-8510 x 223	-called Amanda (Sept. 11 or 12) -called Amanda (Sept. 14) -called Yacine (Oct. 3) -left Yacine a message explaining that he'd like to meet on Oct. 12 with 4 other representatives (Oct. 9) -emailed Yacine with attendance list for his meeting (Oct. 11) -emailed Yacine a written submission in advance of this afternoon's meeting (Oct. 12) -called Yacine to confirm receipt of this document (Oct. 12)	-Letter sent (Sept. 10) NOTE: addressed to Bernard Courtois -Amanda called back (Sept. 12-14?) -Yacine spoke to him by telephone (Sept. 25) -Yacine left him a message (Oct. 2) -Yacine called Bill Munson back and confirmed a Friday, Oct. 12 meeting w/ ITAC and CWTA (Oct. 9)
Terry Patent/OPP Child Pornography Section	(416) 460-6567 (cell) (416) 235-4529	-called Amanda (wk of Sept. 17) -called Yacine back (Oct. 3)	-Letter sent (Sept. 10) NOTE: addressed to Insp. Andy Stewart -Amanda left a message (wk of Sept. 10) -Yacine left a message (Sept. 26) -Yacine called him (Oct. 3)
Michael Geist/University of Ottawa	(613) 562-5800 x 3319	-called Amanda (Sept. 10) -called Yacine (wk of Sept. 17) -called Yacine (Sept. 25) -called Yacine to schedule in-person meeting (Oct. 10)	-Letter sent (Sept. 10) -Yacine called (wk. of Sept. 17) -Yacine left a message (Sept. 25) -Yacine left a message (Oct. 2) -Yacine left a message confirming date and time of meeting (Oct. 12) -Yacine left a message re-confirming time and place (Oct. 17)
John Boufford/Canadian Information Processing Society	(705) 292-5874	-John called Yacine (Sept. 13)	-Letter sent (Sept. 10) -Yacine called John (wk of Sept. 10) -Yacine spoke to him by telephone (Sept. 25) -Yacine left a message (Oct. 2)
Steve Sullivan/Federal Ombudsman for Victims of Crime		-called Public Safety Canada with the aim of being consulted on CNA (Sept. 17)	-Amanda talked to his office (Oct. 2) -Amanda arranged a mtg (Oct. 3)
Alicia Wanless/International Perspectives		-emailed Amanda (Sept. 12) -emailed Amanda (Sept. 14) -emailed Amanda (Oct. 2) -emailed Amanda to say she wants to meet and submit	-Letter sent (Sept. 10) -Amanda wrote email (Sept. 14) -Amanda wrote email (Oct. 2)

		written comments (Oct. 4)	
Paul-Andre Comeau/School of Public Service			-Letter sent (Sept. 10) -Yacine called (wk of Sept. 10) -Yacine called and left a message (Oct. 9)
David Elder/Bell	613-785-6314	-David's assistant called and said to email him (Oct. 9)	-Letter sent (Sept. 10) -Yacine emailed him (Oct. 9) -Yacine emailed him re "thank you" letter (Nov. 23)
Peter Barnes/CWTA		-Keith McIntosh called Yacine to confirm written submission as well as joint meeting with ITAC and Chamber of Commerce (Oct. 5) -submitted their written comments via email (Oct. 12)	-Letter sent (Sept. 10) -Yacine left a message (Oct. 2) -Yacine left a message to confirm CWTA attendance at the Oct. 12 mtg with ITAC (Oct. 9)
Tom Copeland/CAIP	**(905) 373-9313**	-Tom called Yacine back (Oct. 9)	-Letter sent (Sept. 10) -Yacine left him a message (Oct. 2) -Yacine left him a message (Oct. 9) -Yacine called him to confirm CAIP representation for purpose of "thank you" letter (Nov. 29)
Heidi Illingworth/CRCVC		-left a message for Yacine (Oct. 3) re: rescheduled mtg -called Yacine to confirm mtg and establish contact for sending in comments (Oct. 9)	-Letter sent (Sept. 10) -Yacine spoke to her (wk of Sept. 24) -Yacine spoke to her (Oct. 2) to schedule mtg -Yacine left a message (Oct. 3) to reschedule mtg -Yacine called her to confirm numbers (Oct. 9)
Peter Martin/Dep. Com. RCMP			-Letter sent (Sept. 10)
Kim Devooght/IBM Canada	(613) 249-2133		-Jamie called him (wk of Sept. 24??)
Michael Murphy/Canadian Chamber of Commerce	(613) 238-4000 ext. 236	-Michael called Amanda (wk of Sept. 10) -Chris Gray called Amanda to confirm written submission (Oct. 4)	-Amanda left a message (Oct. 3)
Milos Jancik/Electro-Federation of Canada	(905) 602-8877		-Amanda left a message (Oct. 3) -Yacine left a message (Oct. 9)
Canadian Advanced Technology Alliance	(613) 236-6550		-Amanda left a message (Oct. 3)
Edouard Trepanier/Videotron		-Edouard called Yacine to confirm that he had not had time to read the document, will submit written comments based on the website's consult doc. (Oct. 12)	-Jamie called inviting to consultations (Oct. 3) -Yacine left a message (Oct. 9)

		-a representative from M. Trepanier's office called to return Jamie's call to Videotron. Yacine explained that M. Trepanier agreed to a written submission and forwarded the web address of the consultation document to her. (Oct. 15) -Edouard's assistant emailed Yacine to confirm that they would not be providing written comments at this time. They advised us to keep them posted, and said they would participate at a later date (Oct. 16) -emailed Yacine to say they would not be submitting written comments (Oct. 16)	
Ed Prior/Telus	(416) 279-7523		-Jamie called inviting to consultations (Oct. 3) -Yacine called to ask about next steps (Oct. 9)
Kim Devooght/IBM Canada		-Kim called Yacine to notify of his intention to attempt a written submission, and to say that he cannot meet in-person (Oct. 12)	-Jamie called soliciting contact info and return call (wk of Sept. 17) -Jamie called inviting to consultations (Oct. 3) -Yacine left a message (Oct. 9)
Asha Gosein/Yahoo		-Asha called Amanda (Oct. 3)	-Amanda called inviting to consult (Oct. 3) -Amanda returned the call (Oct. 3) -Amanda emailed Asha asking what her status was in terms of participating in the consultations (Oct. 16)
Pippa Lawson/CIPPIC		-Pippa emailed Amanda to confirm written submission (Oct. 4) -emailed her written submission to Amanda (Oct. 15)	-Amanda emailed Pippa (Oct. 3)
Kenneth G. Engelhart/Rogers Communications			-Amanda left a message (Oct. 3)

6950-1

DRAFT 30-Oct-07

CNA Consultations – Status and Planning Report

Groups	Method	Timing	Location
Federal Ombudsman for Victims of Crime **Steve Sullivan, Federal Ombudsman for Victims of Crime** **Louis Théorêt**	Meeting and written submission	Wednesday, Oct. 10th @ 1:00 – 2:15pm	269 Laurier 12th Floor, Section D BR D4700 (12ppl)
Canadian Resource Centre for Victims of Crime **Heidi Illingworth** **Darren Graham** **Jenny Love**	Meeting; written submission from CRCVC and NCECC	Wednesday, Oct. 10th @ 2:30 – 4:00pm	269 Laurier 17th Floor, Section B BR B2000 (16/34ppl)

National Child Exploitation Coordination Centre (NCECC) **Earla-Kim McColl, Superintendent** **RCMP NCECC** **Susan Alter, RCMP Legal Counsel**			
Ontario Provincial Police Child Pornography Section ("Project P") **Inspector Andy Stewart** **Terry Patent**	Conference Call	Thursday, Oct. 11th @ 1:00 – 2:30pm	269 Laurier 12th Floor, Section B BR B2600 (22ppl)

Rogers Communications **Pam Dinsmore, VP Regulatory Rogers Cable** **Joel Thorp** **Jean Trembley**	Meeting	Friday, Oct. 12th @ 10:00 – 11:30am	269 Laurier 13th Floor, Section D BR D4400 (20ppl)
Information Technology Association of Canada (ITAC) **Canadian Association of Internet Providers (CAIP)** **Canadian Advanced Technology Alliance (CATA)** **Canadian Wireless Telecommunications Association (CWTA)**	Meeting; written submissions from ITAC and CWTA	Friday Oct. 12th @ 2:30 – 4:00pm	269 Laurier 12th Floor, Section B BR B2600 (22ppl)

David Elder, Bell **Pam Dinsmore, Rogers** **Parke Davis, TELUS** **Fred Nesbitt, Research In Motion** **Kasia Majewski, CWTA**			
Office of Privacy Commissioner of Canada **Raymond D'Aoust, Assistant Privacy Commissioner** **Trevor Shaw, OPC** **Carman Baggaley, OPC** **Lindsay Scotton, OPC** **Hedy Kirkby, OPC** **Patricia Kosseim, OPC**	Meeting	Monday, October 15th @ 2:00 – 3:30pm	269 Laurier 12th Floor, Section B BR B2600 (22 ppl)

Prof. Michael Geist **Canada Research Chair of Internet and E-commerce Law, University of Ottawa**	Meeting and written commentary	Wednesday, Oct. 17th @ 3:00 – 4:00pm	269 Laurier 16th Floor, Section B BR B4200
Alicia Wanless **Executive Director of International Perspectives**	Meeting and Written Submission	Thursday, Oct. 18th @ 2:00 – 3:30pm	269 Laurier 11th Floor, Section A BR A1600 (16ppl)
Yahoo! Canada **Asha Gosein, Legal Manager + additional staff**	Conference Call	Thursday, Oct. 18th @ 11:00 – 12:00pm	269 Laurier 11th Floor, Section A BR A1600 (16ppl)
Cybertip.ca **Signy Arnason** **Lianna McDonald**	Meeting or Conference Call (TBD)	*Never took place	

Canadian Association of Chiefs of Police (CACP) **Clayton Pecknold, Deputy Chief Constable** **Pierre-Paul Pichette, Assistant Director**	Written Submission		
Professor Avner Levin	Written Submission		
Canadian Chamber of Commerce	Written Submission		
Canadian Internet Policy and Public Interest Clinic (CIPPIC)	Written Submission		

Philippa Lawson, Executive Director **Additional written comments from Ian Kerr, Canada Research Chair in Law, Ethics and Technology at the University of Ottawa**			
Canadian Bar Association	Written Submission		
Videotron	Written Submission	(submission never received)	
IBM	Written Submission	(submission never received)	

Still Awaiting Response: **B'nai Brith** **Electro-Federation of Canada** **Professor Paul-Andre Comeau** **Canadian Information Processing Society**			

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

349886
MIN
—
—
5730-1
9-11-2007

SECRET

DATE: NOV 13 2007

6950-13/349886

MEMORANDUM FOR THE MINISTER

MEETING WITH STEVE SULLIVAN, FEDERAL OMBUDSMAN FOR VICTIMS OF CRIME
(For Information)

ISSUE

- Your upcoming meeting with Steve Sullivan, Federal Ombudsman for Victims of Crime, on Tuesday, November 20th, 2007, from 4:30 - 5:00 p.m. at your Parliament Hill Office.

BACKGROUND

- Established in March 2007, the Office of the Federal Ombudsman for Victims of Crime has been meeting with various departments and agencies (e.g. Commissioner of the Correctional Service of Canada; Chairman of the National Parole Board; National Child Exploitation Coordination Centre (NCECC)) to discuss its mandate and promote the concerns and needs of victims of crime. Part of Mr. Sullivan's mandate is to identify emerging and systemic issues that impact negatively on victims of crime.

- In a letter jointly addressed to yourself and your Justice Canada colleague, Minister Nicholson, dated August 31, 2007, Mr. Sullivan emphasized that an immediate focus of his office was Internet facilitated sexual exploitation of children and sought the Government's cooperation in taking steps to address the issue (**TAB A**).

- In a letter dated September 17, 2007, Mr. Sullivan expressed a desire to meet with you regarding "your recent public comments regarding the lawful access consultation process" (**TAB B**). You responded to the request, indicating that your schedule did not permit a meeting at the time (**TAB C**). Your office has arranged for you to meet with Mr. Sullivan on Tuesday, November 20th, 2007.

Canada

CONSIDERATIONS

- Mr. Sullivan is concerned that the perception among many service providers that a warrant is, or should be, required to obtain customer name and address (CNA) information reduces industry assistance to police, thereby hindering the ability of law enforcement to rescue children from abusive situations.

- Mr. Sullivan believes that recent public comments on the need for a warrant to access CNA information are inconsistent with the recommendation made by the Standing Committee on the Access to Information, Privacy and Ethics [ETHI Committee] regarding its review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

PIPEDA Review

- The Government of Canada's response to the findings of the ETHI Committee's review of PIPEDA was tabled on October 17th (**TAB D**).

- The Government's response clarifies that PIPEDA does not require that a warrant or court order be in place before a business provides personal information on a customer to the police or other agencies. This cooperation has always existed between Canadian companies and police to ensure the safety of the public. The response reads as follows:

> *"The government wishes to confirm 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."*[1]

- On October 27, 2007, Industry Canada (IC) announced that public consultations would be held on the implementation of the Government of Canada response. Views will be sought on, among other things, the concept of "lawful authority". The Department, in consultation with the

---

[1] In a letter to Tom Wappel, Chairman of the ETHI Committee (dated April 19, 2007), you underscored the meaning of section 7(3)(c.1) of PIPEDA: "A requirement to obtain a warrant was never intended, nor would it be practical, given the broad definition of personal information." (**TAB E**). The Government response is consistent with this.

RCMP, will provide input to IC on alternate wording before the January 15, 2008 deadline.

Public Consultations on Access to CNA Information

- On October 10, 2007, Mr. Sullivan met with officials as part of the public consultations on access to CNA information. Mr. Sullivan stated that access to CNA information was a vital tool for law enforcement and should not be subject to judicial pre-authorization. Particular emphasis was placed on the necessity of CNA information for law enforcement in the pursuit of online child sexual exploitation investigations (written submission at **TAB F**).

- Mr. Sullivan will likely advocate the need for legislation requiring telecommunications service providers to provide CNA information to law enforcement for Internet-facilitated child sexual abuse investigations. He may raise concerns in light of your recent public statements on the issue of warrant requirements for police or CSIS access to CNA information, as reported in the media.

PROPOSED TALKING POINTS

- Important work continues to be done in the area of supporting lawful access to communications for law enforcement purposes. Officials are reviewing the consultation submissions, including your own.

- I am committed to an approach that provides law enforcement with access to CNA information, while respecting the privacy interests of individuals and victims of crime.

- I would invite your office to participate in the public consultations on the implementation of the Government Response to the findings of the ETHI Committee's review of PIPEDA.

- Are there crimes, in addition to child exploitation, that have significant victim implications and where police access to CNA information is important?

Suzanne Hurtubise

Enclosures: (6)

Government of Canada
Federal Ombudsman for Victims of Crime
240 Sparks Street
P.O. Box 55037
Ottawa, Ontario
K1P 1A1

Gouvernement du Canada
L'ombudsman fédéral des victimes d'actes criminels
240, rue Sparks
C.P. 55037
Ottawa (Ontario)
K1P 1A1

August 31, 2007

The Honourable Rob Nicholson
Minister of Justice and
Attorney General Canada
284 Wellington St.
Ottawa, ON
K1P 1A1

The Honourable Stockwell Day
Minister of Public Safety
269 Laurier Avenue West
Ottawa, ON
K1A 0P8

Dear Minister Nicholson and
Dear Minister Day:

Since my appointment as Federal Ombudsman for Victims of Crime in April, I have been busy meeting with various departments and agencies within the federal government, as well as with NGOs and academics, in order to discuss our mandate and promote the concerns and needs of victims of crime. Some of these departments and agencies include the Commissioner of the Correctional Service of Canada, the Chairman of the National Parole Board, the National Child Exploitation Coordination Centre, the RCMP Human Trafficking Unit, the Chairman of the RCMP Complaints Commission, the Chairman of the Military Police Complaints Commission and the Department of Foreign Affairs and International Trade.

We have also been developing our complaint process to address concerns of victims and our focus is on trying to find quick resolutions. In fact, we have already had some success assisting an individual who filed a complaint regarding the Correctional Service of Canada. We continue to assist many other victims in identifying the appropriate resources for them to address their particular problems.

As part of our mandate to identify systemic issues that impact negatively on victims of crime, we have undertaken a thorough, victim-centred review of the *Corrections and Conditional Release Act*. This fall, we will be hosting a roundtable with victims groups to identify some key issues. We also gave a presentation to the CSC Review Panel and submitted a written brief (a copy of which is enclosed). I believe our work will complement their anticipated report.

/...2

Canada

In the area of emerging issues, an ongoing theme of our work over the next three years will be the commercial and sexual exploitation of children. Initially, we plan to focus on the problem of Internet facilitated child sexual exploitation. We will work with key stakeholders to identify policy and legislative changes to enhance the ability of police to identify and rescue children who are being victimized. To this end, we have already written to the Minister of Industry encouraging him to consider a recommendation from the Standing Committee on Access to Information, Privacy and Ethics which would clarify and enhance the role of Internet Service Providers to assist law enforcement in their efforts to protect child victims.

A longer term issue is identifying the unique challenges these children face as they grow older. Not only do they have to deal with the sexual abuse itself, but also with the increased trauma of knowing the sexual abuse images are on the Internet forever, for anyone to access. Although there has been a lot of focus on privacy, the Supreme Court did say in *R. v. Sharpe*, that "the privacy of those who possess child pornography is not the only interest at stake in this appeal. The privacy interests of those children who pose for child pornography are engaged by the fact that a permanent record of their sexual exploitation is produced."

Finally, as you both know, all federal, provincial and territorial Ministers of Justice signed the *Canadian Statement of Basic Principles for Victims of Crime* in 2003. The first statement was adopted in 1988. This document is an important part of our mandate and over the next three years, we will be promoting it within the federal government to raise awareness about the Government's responsibilities to victims of crime.

As 2008 marks the 20th anniversary of the original *Canadian Statement of Basic Principles for Victims of Crime* and the 5th anniversary of the 2003 statement, I believe it would be appropriate for the federal government to re-affirm its commitment to these principles via a motion in the House of Commons during the 2008 National Victim Awareness Week. This would remind Canadians of the support this Government continues to show to victims of crime.

I understand you will be meeting with your provincial and territorial counterparts in October and this may afford an opportunity to seek support for their reaffirmation in their respective jurisdictions as well.

/...3

I look forward to meeting with you both in the fall to discuss the work we have been doing and will be doing in the future.

Thank you.

Sincerely,

Steve Sullivan
Federal Ombudsman for Victims of Crime
www.victimsfirst.gc.ca

Cc Ms. Catherine Kane, Director, Policy Centre for Victims of Crime

Government of Canada / Gouvernement du Canada

Federal Ombudsman for Victims of Crime / L'ombudsman fédéral des victimes d'actes criminels

240 Sparks Street
P.O. Box 55037
Ottawa, Ontario
K1P 1A1

240, rue Sparks
C.P. 55037
Ottawa (Ontario)
K1P 1A1

September 17, 2007

The Honourable Stockwell Day
Minister of Public Safety
Room 19A-7400
269 Laurier Avenue West
Ottawa, Ontario
K1A 0P8

Dear Minister Day:

As the Federal Ombudsman for Victims of Crime I am writing to express my concern about your recent public comments regarding the lawful access consultation process (Day firm on police warrants for access to internet user data, September 14, 2007.)

Currently, some Internet Service Providers (ISPs) provide basic customer information (i.e. name and address) without a warrant to law enforcement agencies investigating Internet facilitated child sexual abuse. Unfortunately, not all ISPs cooperate without a warrant. In light of your comments, there is a growing concern that those ISPs who are cooperating will stop doing so, the impact of which could be devastating not only for law enforcement agencies but more so for the child victims. Your department's consultation document states, "The availability of such building-block information is often the difference between the start and finish of an investigation."

Your comments are in contradiction to the recommendation made by the Standing Committee on the Access to Information, Privacy and Ethics regarding its review of the *Personal Information Protection and Electronic Documents Act (PIPEDA). Recommendation #12*, states,

> *"The Committee recommends 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 [...]"*

The Committee agreed that it is not realistic or necessary to expect police to seek a warrant in these situations for basic information such as a name and address.

Canada is a signatory to several key UN declarations that speak to the need to protect and promote the safety and privacy of victims and children. In 2003, the Government of Canada signed the *Canadian Basic Statement of Principles for Victims of Crime*, which commits the federal government to consider and respect the privacy of victims to the greatest extent possible, to minimize inconvenience to victims and to take appropriate measures to protect victims.

Canada

More recently, Canada with other G8 Ministers agreed to accelerate efforts to combat child sexual exploitation. The G-8 Ministers committed, "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."[1] The Ministers also acknowledged and recognized that the private sector, including Internet Service Providers (ISP), have a role to play in protecting the world's children.

In the 2007 Budget, the Government of Canada committed an additional $6 million to protect children from sexual exploitation. The Honourable Jim Flaherty, Minister of Finance stated, "The funding will ensure that those who commit these heinous offences are brought to justice..."[2]

Last week, the privacy community raised concerns about the privacy implications to customers, although it must be made clear that the information the police are seeking at this stage (i.e. name and address) is not invasive. Unfortunately, no one spoke about the privacy implications for children who are victims of internet sexual exploitation. Our Office believes there is no greater violation of one's privacy than having images of rape and abuse traded like baseball cards on the internet.

There are over a million images of child sexual abuse available on the Internet, involving tens of thousands of children. The child sexual abuse images are getting more violent and the children in the photos are getting younger. New victims are appearing every week. As the G-8 Ministers said, "Child pornography grievously harms all children: it harms the child who is sexually assaulted in the making of the image; the same child is re-victimized every time that image is viewed."[3]

As the first Federal Ombudsman for Victims of Crime, I was given a mandate to ensure the Government meets its responsibilities to victims of crime. I am therefore asking you to reconsider your position. The current law leaves children vulnerable to further abuse, as it interferes with the ability of law enforcement to potentially rescue children from abusive situations.

I am willing to personally meet with you to discuss this issue further.

Sincerely,

Steve Sullivan
Federal Ombudsman for Victims of Crime

---

[1] G-8 Justice and Home Affairs Ministers, May 24, 2007. www.g8.gc.ca/childpornography-en.asp
[2] Ibid

Minister of Public Safety | Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

OCT 15 2007

Mr. Steve Sullivan
Federal Ombudsman for Victims of Crime
240 Sparks Street
P.O. Box 55037
Ottawa, Ontario K1P 1A1

Dear Mr. Sullivan: Steve

Thank you for your correspondence of September 17, 2007, in which you request to meet with me, regarding my public comments concerning the lawful access consultation process.

Unfortunately, prior commitments prevent me from meeting with you at this time. I understand that you have met with departmental officials on Wednesday, October 10, 2007. Please rest assured that your input is being carefully considered, alongside that of other parties, as part of the consultations.

Thank you again for taking the time to write on this important issue.

Yours sincerely,

Stockwell Day, P.C., M.P.
Minister of Public Safety

Steve, this is important stuff. Let's try to get together in the near future, after I've gone over your and others' concerns on this.

Ty S.

Canada

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)

Government of Canada Gouvernement du Canada

Canada

Mr. Tom Wappel, M.P.
Chair
Standing Committee on Access to Information, Privacy and Ethics
House of Commons
East Block, Room 115
Ottawa, Ontario K1A 0A6

Dear Mr. Wappel:

Pursuant to *Standing Order 109 of the House of Commons*, I am pleased to respond on behalf of the Government of Canada to the recommendations made by the House of Commons Standing Committee on Access to Information, Privacy and Ethics in its report on the Statutory Review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), tabled in the House on May 2, 2007.

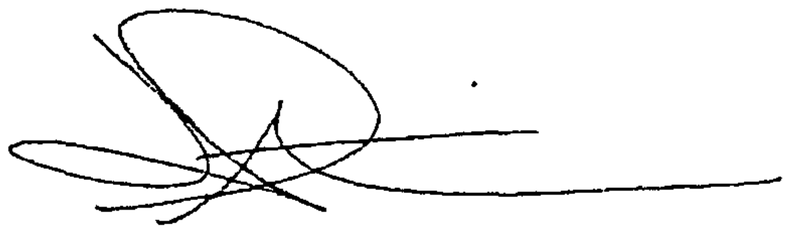
The Government of Canada extends its gratitude to the members of the Committee for their comprehensive review of PIPEDA. The Committee's thoughtful recommendations provide valuable guidance as the government continues to ensure that personal information is protected in a manner that reflects both the values of individual Canadians, as well as the needs of business in the information age.

The government would also like to express its appreciation to the many stakeholders, including the Privacy Commissioner of Canada, privacy advocates, law enforcement and victim groups, industry associations and individual businesses who appeared as witnesses and provided written submissions to the Committee. The views expressed throughout the review offer valuable insight as to how PIPEDA has functioned throughout its first five years of existence, and how its effectiveness can be improved going forward.

Overall, the government shares the Committee's observation that PIPEDA is not in need of significant change at this time. The Committee report usefully points to a few specific areas where the Act can be improved. Of equal importance however, the Committee has highlighted the need for greater education and awareness of privacy protection among both individuals and businesses.

I look forward to consulting further on a number of issues raised during the Review, including the proposed legislative improvements that will ensure that PIPEDA continues to merit its long-standing reputation as a world-class model for the protection of personal information in the private sector.

Sincerely,



Jim Prentice
Minister of Industry

Government Response to the Fourth Report of the Standing Committee on Access to Information Privacy and Ethics

In May 2007, the Standing Committee on Access to Information, Privacy and Ethics ("the Committee") concluded its review of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), pursuant to section 29 of the Act. During the process of the review, the Committee heard from 67 witnesses and considered 34 submissions from individual Canadians and Canadian organizations. In its Report, the Committee presented 25 recommendations to the government, addressing key issues raised during the review. The government has taken full account of the Committee's Report and its recommendations, as well as the full range of opinion presented as part of the Parliamentary Review, in considering what actions might be taken in relation to the Act and its implementation.

The Report of the Parliamentary Committee, consistent with the submissions it received, has underlined the critical importance of an effective legal framework for the protection of personal information in Canada. As the Committee points out, privacy represents a fundamental value for Canadians, and the management and use of personal data is crucial to the conduct of business, trade and commerce in a modern, information-driven global economy.

Moreover, the importance of privacy protection has dramatically increased in recent years with the emergence of the Internet and online commerce. As of 2005, 68% of Canadians use the Internet, and more than 82% of Canadian businesses are now online. According to Statistics Canada, the total value of online commerce in Canada in 2006 was $49.9 billion. These developments have thus greatly enlarged the capacity to collect, transfer, and process large quantities of personal information, creating new challenges for both industry and governments. Consequently, more than ever before, consumers and businesses can benefit from clear and effective safeguards for protecting and securing personal data, especially in relation to online business and electronic commerce.

Canada has responded well to these challenges. Internationally, Canada's privacy regime is recognized as one of the best in the world. In 2001, the European Commission recognized PIPEDA as providing "adequate" privacy protections for the purposes of the EU Data Protection Directive, thereby allowing the personal information of Europeans to enter into Canada without restrictions. In a 2006 study by Privacy International, a privacy advocacy group located in Great Britain, Canada's privacy regime was ranked second only to Germany in a survey of 37 countries. In particular, PIPEDA, alongside related federal and provincial legislation, has achieved an appropriate balance between privacy protection and the efficient management and use of information in a business environment.

We agree with the Committee that radical changes to the legislation are not warranted at this time, especially in light of the relatively short period of time the Act has been fully in force. The government further agrees with the Committee on the need and value of "fine tuning" the legislation and its implementation in a manner that strengthens the overall effectiveness of privacy protection in Canada. In this respect, the Committee's proposals for selective legislative changes and other actions are extremely helpful. In particular, the government commends those recommendations that are especially designed to:

- improve clarity and certainty with respect to key definitions and provisions in the Act;
- increase education and awareness of privacy protection measures among individual Canadians and organizations, especially small businesses; and
- maintain a flexible, "light-handed" approach to privacy regulation and oversight.

The government is committed to protecting the privacy of Canadians and, in concert with other interested parties, will take whatever steps are necessary to ensure Canada's laws and policies are meeting the highest possible standard of privacy protection. To this end, the government has reviewed the Committee's general findings and each individual recommendation of the Committee, noting below those which it believes merit priority attention in future work.

Response to Recommendations

The following section addresses each of the Committee's recommendations individually, pointing to where the government agrees with the Committee's conclusions either in whole or in part, and to those issues where further work or consultation is required.

Business Contact Information

Recommendation 1

"The Committee recommends that a definition of 'business contact information' be added to PIPEDA, and that the definition and relevant restrictive provision found in the Alberta *Personal Information Protection Act* be considered for this purpose."

Response

This recommendation reflects the widespread view expressed to the Committee that the current approach to "business contact information" in PIPEDA is too narrow and is, therefore, inadequate in meeting the requirements for business communications in the information age. The government agrees that an amended definition of "business contact information", which is inclusive of business email and fax numbers, and which is sufficiently broad to account for changes in communications technologies, could provide more certainty about the business use of this type of data without detracting from the protections given to other types of personal information.

In this regard, the government will explore ways in which the protections established in the Alberta *Personal Information Protection Act* for business contact information can be incorporated into PIPEDA in such a way as to ensure that business contact information is excluded only if collected, used or disclosed for the purposes of contacting an individual in their business capacity.

Work Product Information

Recommendation 2

"The Committee recommends that PIPEDA be amended to include a definition of 'work product' that is explicitly recognized as not constituting personal information for the purposes of the Act. In formulating this definition, reference should be made to the definition of 'work product information' in the British Columbia *Personal Information Protection Act*, the definition proposed to this Committee by IMS Canada, and the approach taken to professional information in Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector*."

Response

The government recognizes that the issue of work product information is of great significance to a number of stakeholders. In its Report, the Committee has acknowledged the call from private sector interests to provide more clarity and certainty to PIPEDA in this area in order to facilitate business planning and to assist them in their efforts to comply with the Act.

At the same time, the government must consider the concerns expressed by the Privacy Commissioner and others regarding the risk of any

unintended negative consequences to privacy that may result from an exemption of work product information.

In keeping with the general approach of PIPEDA, it is important to balance the need for a business-friendly privacy regime with the need for maintaining the existing level of privacy protection currently provided by the Act. In light of this, the government will commit to consult further and consider how organizational needs respecting collection, use, and disclosure of work product information can be accommodated in a manner that poses the least degree of risk to privacy protection.

As proposed by the Committee, consideration will be given to various approaches, including those proposed in submissions to the Committee and those contained in provincial privacy laws.

Destruction of Data
Recommendation 3

"The Committee recommends that a definition of 'destruction' that would provide guidance to organizations on how to properly destroy both paper records and electronic media be added to PIPEDA."

Response

The government notes the Committee's recommendation to include a definition of "destruction" in PIPEDA. Recognizing a need for greater clarity in this area, a variety of provisions already exist within PIPEDA that provide direction pertaining to the destruction of personal information.

Consequently, it may be sufficient to develop non-legislative guidance to further assist organizations in disposing of personal information in accordance with PIPEDA's existing requirements. The government will work with the private sector and with other stakeholders to develop tools that can provide organizations with further clarity in this area.

Consent: General Principles
Recommendation 4

"The Committee recommends that PIPEDA be amended to clarify the form and adequacy of consent required by it, distinguishing between express, implied and deemed/opt-out consent. Reference should be made in this regard to the Alberta and British Columbia *Personal Information Protection Acts*."

Response

The Government of Canada fully acknowledges the importance of meaningful consent to effective privacy protection. To this end, PIPEDA establishes a flexible legislative approach that takes into account the divergent needs and practices of the many organizations it captures.

In accordance with her mandate to develop information products to educate the public on the Act and its purposes, the Privacy Commissioner of Canada has produced guidance material that aims to assist organizations in better understanding and implementing PIPEDA's consent requirements.

To supplement these valuable tools, the government commits to consulting with stakeholders to identify possible areas where further guidance may be necessary, and develop tools in this respect. The government would welcome the participation of the Privacy Commissioner of Canada and her provincial counterparts in these and similar efforts.

Consent: Employee/Employer Relationship
Recommendation 5

"The Committee recommends that the Quebec, Alberta and British Columbia private sector data protection legislation be considered for the purposes of developing and incorporating into PIPEDA an amendment to address the unique context experienced by federally regulated employers and employees."

Response

The government agrees with the Committee's recommendation and with a number of stakeholders, including the Privacy Commissioner of Canada, regarding the need to better account for the unique circumstances regarding consent in employee/employer relationships.

In studying privacy protection for employees of federally regulated organizations, consideration should be given to the provisions in the laws of Quebec, British Columbia and Alberta, as well as the recommendations of the Privacy Commissioner, to ensure that the privacy rights of employees continue to be protected under PIPEDA.

Investigative Bodies
Recommendation 6

"The Committee recommends that PIPEDA be amended to replace the 'investigative bodies' designation process with a definition of 'investigation' similar to that found in the Alberta and British Columbia *Personal Information Protection Acts* thereby allowing for the collection, use and disclosure of personal information without consent for that purpose."

Response

The government recognizes that the current process for designating investigative bodies has proven to be lengthy and cumbersome for applicants who need this designation under the Act to conduct investigations. The government also agrees with the Committee that the lack of consistency in s. 7 of PIPEDA with respect to exemptions for collection, use and disclosure of personal information is a source of frustration for some organizations in their efforts to detect and prevent fraud, particularly within the financial sector. However, consideration must also be given to the support expressed by the Privacy Commissioner and privacy advocates for the transparency of the current process, which provides for a public listing of designated organizations.

However, further consideration is required on the best alternative to the current process of designation. The government agrees that there is merit in examining the approaches taken by Alberta and British Columbia, which define the term "investigation" and allows collection, use and disclosure without consent for that purpose. In addition to making the process more efficient, and in accordance with the Government of Canada's Paperwork Burden Reduction Initiative, this approach would allow greater harmonization with the provinces. Therefore, the government will give further consideration the issue of how best to streamline the Act's provisions in respect of private sector investigative activity.

Business Transactions
Recommendation 7

"The Committee recommends that PIPEDA be amended to include a provision permitting organizations to collect, use and disclose personal information without consent, for the purposes of a business transaction. This amendment should be modelled on the Alberta *Personal Information Protection Act* in conjunction with enhancements recommended by the Privacy Commissioner of Canada."

Response

The government agrees with the recommendation, which reflects a general consensus among those who appeared before the Committee that PIPEDA should be modified to allow organizations to collect, use and disclose personal information as necessary for the conduct of business transactions, such as mergers and acquisitions.

The Alberta and British Columbia *Personal Information Protection Acts* provide models that can be drawn upon to accommodate the information needs of organizations engaged in business transactions while ensuring that individuals' personal information continues to be protected.

Principal-Agent Relationships
Recommendation 8

"The Committee recommends that an amendment to PIPEDA be considered to address the issue of principal-agent relationships. Reference to section 12(2) of the British Columbia *Personal Information Protection Act* should be made with respect to such an amendment."

Response

Recognizing the Committee's observation that there may be confusion regarding the application of PIPEDA to situations where organizations engage third parties for activities that involve the collection, use and disclosure of personal information, the government proposes education and guidance as an alternative to legislative amendments. Therefore, the government will work with the Privacy Commissioner and other stakeholders to develop tools to provide further clarity on this matter.

Litigation Process / Legal Proceedings
Recommendation 9

"The Committee recommends that PIPEDA be amended to create an exception to the consent requirement for information legally available to a party to a legal proceeding, in a manner similar to the provisions of the Alberta and British Columbia *Personal Information Protection Acts*."

Response

The government notes the Committee's recommendation and acknowledges that it was made in response to concerns expressed by certain stakeholders regarding the need to ensure that PIPEDA does not impede litigation procedures. However, the government does not share the Committee's view that such an amendment is necessary at this time.

Witness Statements

Recommendation 10

"The Committee recommends that the government consult with the Privacy Commissioner of Canada with respect to determining whether there is a need for further amendments to PIPEDA to address the issue of witness statements and the rights of persons whose personal information is contained therein."

Response

The government agrees with the Committee's recommendation to consult with the Privacy Commissioner, the legal community, as well as other relevant stakeholders, to determine whether an amendment to PIPEDA is needed to address issues of witness statements.

Individual, Family and Public Interest Exceptions

Recommendation 11

"The Committee recommends that PIPEDA be amended to add other individual, family or public interest exemptions in order to harmonize its approach with that taken by the Quebec, Alberta and British Columbia private sector data protection Acts."

Response

The government agrees with the Committee's view that certain limited exceptions to PIPEDA's consent requirements may be warranted in order to address the concerns expressed by stakeholders regarding the disclosure of personal information in cases of natural disasters, elder abuse and other similar circumstances. However, in the interest of maintaining strong privacy protection, any amendment to PIPEDA should be narrowly defined to ensure that it will be used only for the intended purposes.

In considering options, the government will study the approaches taken in the Alberta and British Columbia *Personal Information Protection Acts*, as well as Quebec's legislation, *An Act Respecting the Protection of Personal Information in the Private Sector*.

Law Enforcement / National Security Interests

Recommendation 12

Recommendation 12 contains two related, but distinct, proposals for legislative amendment. The first pertains to the definition of lawful authority, and the second pertains to s. 7(3) and its exceptions from consent for disclosures of personal information.

"The Committee recommends that consideration be given to clarifying what is meant by 'lawful authority' in section 7(3)(c.1) of PIPEDA[.]"

Response

The government considers the safety and security of Canadian citizens to be of utmost importance. In meeting this objective, it firmly believes that the information needs of law enforcement and security agencies can be met while respecting the right of privacy of Canadians.

The government wishes to confirm 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.

The government acknowledges the concerns expressed by those engaged in protecting the safety of Canadians, regarding the current interpretation of s. 7(3)(c.1) by the certain private sector organizations, and the challenges that this has at times

caused to the investigation and prevention of criminal activity in Canada.

The government therefore agrees with the Committee that there is a need to clarify the concept of "lawful authority" for the purposes of s.7(3)(c.1) of the Act.

"[The Committee recommends 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 [...]'"

Response

As noted above, a clearer definition and understanding of what constitutes "lawful authority" would address the current ambiguity regarding organizations' right under PIPEDA to disclose personal information for the purpose of law enforcement or national security. The proposal to include in PIPEDA a further provision designed to require organizations to disclose personal information would be difficult to implement, given that the purpose of PIPEDA is not well-suited to such a requirement. For this reason, the government does not propose to implement this aspect of the Committee's recommendation.

Definition of "Government Institution"
Recommendation 13

"The committee recommends that the term 'government institution' in sections 7(3)(c.1) and (d) be clarified in PIPEDA to specify whether it is intended to encompass municipal, provincial, territorial, federal and non-Canadian entities."

Response

The government recognizes the benefits of providing clarity on the term "government institutions" and notes that a provision already exists in PIPEDA to grant the Governor-in-Council the power to make regulations in relation to such matters. As such, it would be possible to define "government institution" in the Act through regulation.

Industry Canada will examine the possibility of proceeding with a regulation that will further define the term "government institution" for the purposes of the Act.

Section 7(1)(e)
Recommendation 14

"The Committee recommends the removal of section 7(1)(e) from PIPEDA."

Response

The Government of Canada notes the recommendation of PIPEDA arising from the *Public Safety Act, 2002* (s.7(1e)), and acknowledges the concerns expressed by the Privacy Commissioner and others respecting the potential impact of this provision on the privacy of Canadians. However, given the important public safety interests it is designed to address, the government is not prepared to remove s. 7(1)(e) from PIPEDA at this time.

Personal Information of Minors
Recommendation 15

"The Committee recommends that the government examine the issue of consent by minors with respect to the collection, use and disclosure of their personal information in a commercial context with a view to amendments to PIPEDA in this regard."

Response

The government recognizes that the privacy of minors can be vulnerable, particularly in an online environment. In support of the Committee's recommendation, the government will consult with relevant stakeholders to examine the issue of consent by minors, and to consider the necessity and feasibility of amending PIPEDA in this respect.

Transborder Data Flows
Recommendation 16

"The Committee recommends that no amendments be made to PIPEDA with respect to transborder flows of personal information."

Response

While the government agrees with the Committee's recommendation that legislative amendments are not necessary, it is also important to recognize the privacy concerns raised by transborder data flows and the importance of addressing these challenges through international cooperation. As such, the government has long been committed to working with its international counterparts on these matters, and continues to do so. For example, Canada was involved in the conception of the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted in 1980. More recently, Canada participated in the development of the Asia-Pacific Economic Cooperation (APEC) *Privacy Framework* and continues to be actively engaged in cooperative efforts to develop cross-border privacy rules in compliance with the *Framework*. Finally, the government is currently working with Mexico and the United States to address issues of transborder data flows in a North American context through the Security and Prosperity Partnership (SPP).

Personal Health Information
Recommendation 17

"The Committee recommends that the government consult with members of the health care sector, as well as the Privacy Commissioner of Canada, to determine the extent to which elements contained in the PIPEDA Awareness Raising Tools document may be set out in legislative form."

Response

The government welcomes the support expressed by the health care community and other stakeholders for the PIPEDA Awareness Raising Tools (PARTs) document. In concurrence with the Committee's recommendation, Industry Canada will work with Health Canada, the Privacy Commissioner of Canada, the health care community, as well as provincial and territorial governments to discuss the possible options for according the PARTs document more formal status.

Order-Making Powers
Recommendation 18

"The Committee recommends that the Federal Privacy Commissioner not be granted order-making powers at this time."

Response

The government agrees that the Privacy Commissioner should not be granted order-making powers at this time. This position is supported by the general view expressed throughout oral and written submissions to the Committee that PIPEDA is working quite well. In addition, the relatively short time for which the Act has been in existence warrants a cautionary approach to making significant amendments to the enforcement powers of the Privacy Commissioner. Rather, the Commissioner should be given additional time to make full use of the enforcement powers that are currently at her disposal.

Naming Names
Recommendation 19

"The Committee recommends that no amendment be made to section 20(2) of PIPEDA with respect to the Privacy Commissioner's discretionary power to publicly name organizations in the public interest."

Response

The government agrees with the Committee's recommendation that no legislative change is required in this regard. The Privacy Commissioner currently possesses the ability under PIPEDA to publicly name organizations that are subject to complaints, and should retain the discretion to determine when it is in the public interest to use this power.

Sharing Information with Other Data Authorities
Recommendations 20 and 21

Recommendation 20

"The Committee recommends that the Federal Privacy Commissioner be granted the authority under PIPEDA to share personal information and cooperate in investigations of mutual interest with provincial counterparts that do not have substantially similar private sector legislation, as well as international data protection authorities."

Recommendation 21

"The Committee recommends that any extra-jurisdictional information sharing, particularly to the United States, be adequately protected from disclosure to a foreign court or other government authority for purposes other than those for which it was shared."

Response
(to Recommendations 20 and 21)

The government agrees with the need for the Privacy Commissioner to cooperate in multi-jurisdictional investigations. The global nature of the modern economy requires that the Privacy Commissioner be able to work with other authorities responsible for the protection of personal information, both in Canada and abroad, in order to fulfill her mandate under PIPEDA.

It further agrees that the Privacy Commissioner's current power to share information with her counterparts is too limited and therefore constrains her ability to work effectively in this manner. However, any agreements to share information with foreign authorities should include appropriate constraints to stipulate that information only be used in fulfilment of the purposes for which it is shared. This Committee recommendation is directly related to ongoing work within the Organisation for Economic Co-operation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC) and the

Security and Prosperity Partnership (SPP) directed at improving cross-border enforcement of privacy rules. The federal government and the Privacy Commissioner of Canada are both actively involved in these initiatives.

Solicitor-Client Privilege

Recommendation 22

"The Committee recommends that PIPEDA be amended to permit the Privacy Commissioner to apply to the Federal Court for an expedited review of a claim of solicitor-client privilege in respect of the denial of access to personal information (s.9(3)(a)) where the Commissioner has sought, and been denied, production of the information in the course of an investigation."

Response

The government acknowledges the Committee's recommendation in respect of the ability of the Privacy Commissioner of Canada to verify claims of solicitor-client privilege. The government also notes that in October 2006, the Federal Court of Appeal ruled on this matter in *Blood Tribe Department of Health v. the Privacy Commissioner of Canada*. Given that in March 2007, the Privacy Commissioner was granted leave to appeal before the Supreme Court of Canada, the government would submit that any legislative action to address the issue of solicitor-client privilege would be inappropriate at this time and that it will await the decision of the Supreme Court on the matter.

Data Breach Notification

Recommendations 23, 24 and 25

Recommendation 23

"The Committee recommends that PIPEDA be amended to include a breach notification provision requiring organizations to report certain defined breaches of their personal information holdings to the Privacy Commissioner."

Response

The government recognizes that identity theft is a significant and growing problem and that the increasing frequency of large data breaches involving personal information is a contributing factor. It is also recognized that the majority of businesses act in good faith, and notify those affected in the event of breaches as a matter of course. Some, however, do not. In this light, the government agrees with the Committee that a legislative requirement for notification of data breaches would establish a consistent approach across the marketplace and encourage all organizations to take the security of personal information seriously.

As the Committee's Report acknowledges, public notification of data breaches is a complex issue with significant implications for organizations and individuals. There is a general recognition of the need in certain circumstances for notification to individuals or organizations who are impacted by a breach so that they can take steps to mitigate their risk of harm. However, as many breaches pose no real threat to the personal information of individuals, a requirement for public notification in all cases would be burdensome and costly to organizations and might even diminish its value to the public (through notification "fatigue"). Therefore, in the case of certain defined breaches, where a high risk of significant harm to individuals or organizations exists, the government supports a legislative requirement for the prompt notification of those affected by the loss or theft of personal information.

In addition, as the Committee recommends, a requirement to report any major loss or theft of personal information to the Privacy Commissioner of Canada within a specified time-frame, including the details of the incident and steps taken by the organization to notify individuals (or justification for not doing so), would allow for oversight of organizational practices. This will allow the Privacy Commissioner an opportunity to track the volume and nature of breaches, and the steps taken by organizations respecting the notification process when required. This would be particularly useful to small and medium-size enterprises (SMEs) that may lack the internal resources necessary to make notification assessments.

Recommendation 24

"The Committee recommends that upon being notified of a breach of an organization's personal information holdings, the Privacy Commissioner shall make a determination as to whether or not affected individuals and others should be notified and if so, in what manner."

Response

The decision as to whether or not individual notification is required in the event of a breach must be based on an analysis of the level of risk of harm on a case-by-case basis. Assuming appropriate oversight by the Privacy Commissioner of Canada, the organization experiencing the breach is well positioned to understand and assess the risks involved and to make a prompt determination regarding whether and how to proceed with notification of their customers, business partners, and/or the general public. Assigning the Privacy Commissioner the responsibility to decide on notification, as proposed by the Committee, would be a less effective alternative, as well as more burdensome for that Office from a resource perspective.

Recommendation 25

"The Committee recommends that in determining the specifics of an appropriate notification model, consideration should be given to questions of timing, manner of notification, penalties for failure to notify, and the need for a 'without consent' power to notify credit bureaus in order to help protect consumers from identity theft and fraud."

Response

The government recognizes that the determination of the specifics of the model, including "triggers" and "thresholds" for notification (to both the Privacy Commissioner and affected individuals) will be a critical element in the breach notification provision. Research, analysis and consultation will be required to arrive at the best model for Canada.

An important part of consultations will pertain to specifics for the purpose of developing effective and practical notification parameters as well as for the purpose of determining whether specific offences are appropriate. The issues considered will include the timing, form, content and mode of notification to individuals, and in addition, identification of which organizations, such as credit bureaus, should be notified in addition to the Privacy Commissioner. Clearly defined, industry-wide guidelines and standards would be particularly useful to SMEs that may lack the internal resources necessary to make notification assessments.

Conclusions and Next Steps

In a modern, information-based economy, a solid, efficient regime for the protection of personal information is vitally important for both consumers and businesses. For this reason, the government is committed to ensuring that Canadians continue to benefit from one of the highest standards of privacy protection in the world. It further recognizes the valuable role of PIPEDA in meeting this objective, and the importance of fine-tuning the Act where necessary.

The ETHI Report underlines the complexity and sensitivity surrounding many of the issues that relate to Canada's laws and policies for the protection of personal information. The government appreciates the efforts of the Committee in developing proposals for consideration which will significantly advance the goal of improving the legislation and its implementation. While stating its position on many of the ETHI recommendations, the government believes further work and consultation is needed in several critical areas before a full range of legislative and policy proposals can be presented for parliamentary consideration.

In moving forward, the government intends to conduct further consultations to ensure that any changes to PIPEDA and its implementation are the most effective possible. The government will consult with the Canadian public, other government departments and agencies, as well as provincial and territorial governments, and will take special note of the views of the federal Privacy Commissioner.

Further consultations will help establish a consensus with respect to issues where disagreement exists. In areas where a general consensus exists, consultations can help determine how they could be most effectively implemented. This process will also provide a final opportunity to raise any issues not reflected in the Committee's Report, and seek to address concerns expressed by law enforcement and national security agencies with respect to provisions in PIPEDA designed to protect their investigations.

Lastly, the public consultations will allow provincial and territorial governments to provide input into the review process, as changes to PIPEDA will have implications for the protection of privacy in all provinces and territories.

On the basis of the views received, the government will return to Parliament in the near future with specific proposals for both legislative and non-legislative action.

Minister of Public Safety and Emergency Preparedness

Ministre de la Sécurité publique et de la Protection civile

Ottawa. Canada K1A 0P8

19 APR 2007

Mr. Tom Wappel, M.P.
Chairman
Standing Committee on
Access to Information, Privacy and Ethics
House of Commons
Ottawa, Ontario K1A 0A6

***Re: Statutory Review of the Personal Information Protection and Electronic Documents Act* (PIPEDA)**

Dear Mr. Wappel:

Thank you for your letter of March 20, 2007. I appreciate the opportunity to contribute to the House of Commons Standing Committee on Access to Information, Privacy and Ethics' important work in conducting a statutory review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

You requested my views on s. 7(1) (e) of PIPEDA, which was added to PIPEDA by the *Public Safety Act.*

Subsection 7(1)(e) provides that an organization may collect personal information without the knowledge or consent of the individual if the collection is made for the purposes of a disclosure required by law or a disclosure to the government, where the information relates to national security, defence, or international affairs and is either requested by a government institution that has lawful authority to obtain it, or on the organization's own initiative.

Part of the objective of subsection 7(1)(e), as part of the *Public Safety Act* (which received Royal Assent on May 6, 2004), is to improve Canada's capacity to provide a secure environment, in particular for transportation and air travel. The Act closes legislative gaps relating to transportation and national security by amending existing laws, such as the *Aeronautics Act*, the *Criminal Code*, the *Canadian Air Transport Security Authority Act,* and others, as well as PIPEDA.

The amendments to the *Aeronautics Act* in particular were designed to grant the authority to request, and use, passenger information to protect the security of the country and its aviation system. The amendments to PIPEDA s.7 (1) (e) and 7(2) (d) were consequential amendments needed to ensure that the provisions of PIPEDA did not conflict with the *Public Safety Act*.

It should also be noted that an important goal of the *Public Safety Act* is to balance the interest of public safety and individual privacy, and a number of safeguards were included in the law to achieve this, while ensuring transparency and accountability. The proposals were the subject of extensive consultations, and a lengthy review in Parliament. Many changes were made throughout this process to address comments and concerns expressed by various stakeholders, including the Office of the Privacy Commissioner and, as a result, the amendments to PIPEDA provided for under s. 98 of the *Public Safety Act* are limited in scope and narrowly targeted to achieve their goals.

Given the above, I am concerned about the impact that changes suggested by witnesses to the previous PIPEDA amendments, enacted pursuant to the *Public Safety Act*, could have on achieving the goals of the *Public Safety Act* and, as a consequence, on public safety.

Strong safeguards in relation to law enforcement activities are already enshrined in legislation such as Police Acts and the *Criminal Code*, to review the actions of the police when collecting and using personal information. In addition, the court system oversees the results of police work and ensures, in applying the laws of evidence, as well as the *Charter of Rights and Freedoms*, that police collection of information is done appropriately.

As you know, PIPEDA was enacted to protect the privacy of information being held by private companies and was never intended to impede police work. However, the current wording of section 7 and section 9 of PIPEDA has led to confusion among the private sector as to how and whether they can cooperate with the police, which should be remedied.

<u>Section 7:</u>

Subsection 7(3)(c.1) states that an organization may disclose personal information without the knowledge or consent of the individual if the government institution has lawful authority to obtain the requested information. Unfortunately, the phrase "lawful authority" has been misinterpreted by some private sector organizations as an obligation to obtain judicial authorization before releasing any information to police and security agencies.

While the language of s.7(3)(c), which refers to subpoenas and warrants, can clearly be considered to preclude such an interpretation of lawful authority under s.7(3)(c.1), the reality is that the lack of a definition of lawful authority has resulted in an ambiguity, which is in many instances posing a problem for police. A requirement to obtain a warrant was never intended, nor would it be practical, given the broad definition of personal information. This misinterpretation can result in an inability for police to obtain even basic information needed for general policing functions to assist the public. A troubling example of the potential negative impact of a misinterpretation of this provision is seen in the context of an Internet Service Provider refusing to provide urgently necessary contact information on a subscriber to the police in a situation where a child is being lured in real-time in a chat room by an online predator.

Given the above challenges resulting from the lack of clarity as to what constitutes "lawful authority", I believe that this section, in particular the term "lawful authority", would benefit from clarification.

<u>Section 9:</u>

Section 9 of PIPEDA is also causing law enforcement agencies some concern, due to a possible loophole in the provision designed to protect police investigations. PIPEDA provides that an individual shall be given access to personal information about themselves and have a right to be informed about the disclosure of any of their personal information. To protect investigations, section 9 of PIPEDA provides an exception whereby law enforcement agencies can object and thereby prohibit an organization from revealing to an individual that a request has been received from or disclosure of information has been provided to a law enforcement agency.

Section 9, however, does not address the situation where an organization chooses voluntarily to disclose to an individual a police request for information. Significant harm can result to ongoing police investigations if an organization voluntarily discloses to an individual that he or she is under investigation. For example, this individual or group could then proceed to destroy evidence before the police could intercede.

It is therefore important to police investigations that section 9 be clarified to ensure that organizations are prohibited from disclosing the existence of an investigation or the fact that the police had made any inquiries regardless of

whether an individual has made a request for this information or the organization wishes to voluntarily notify the individual.

I recently wrote to my colleague, the Honourable Maxime Bernier, Minister of Industry, to advise him of the challenges the police have experienced with respect to PIPEDA. I have attached a copy of my letter to him for your reference.

Thank you again for the opportunity to contribute to the Committee's work in reviewing this important piece of legislation.

Yours sincerely,

Stockwell Day, P.C., M.P.
Minister of Public Safety

Federal Ombudsman for Victims of Crime Submission to the CNA Data Consultation Panel

October 10, 2007
Ottawa, Canada

FEDERAL OMBUDSMAN FOR VICTIMS OF CRIME
SUBMISSION TO CNA DATA CONSULTATION

The Office of the Federal Ombudsman for Victims of Crime was announced in March, 2006 by the Minister of Justice and the Minister of Public Safety. The mandate of the Federal Ombudsman for Victims of Crime relates exclusively to matters of federal responsibility and includes:

- facilitate access of victims to existing federal programs and services by providing them with information and referrals;
- address complaints of victims about compliance with the provisions of the *Corrections and Conditional Release Act (CCRA)* that apply to victims of offenders under federal supervision and provide an independent resource for those victims;
- enhance awareness among criminal justice personnel and policy makers of the needs and concerns of victims and the applicable laws that benefit victims of crime, including to promote the principles set out in the *Canadian Statement of Basic Principles of Justice for Victims of Crime*; and
- identify emerging issues and exploring systemic issues that impact negatively on victims of crime.

As part of our duty to alert the Government to emerging issues that impact negatively on victims of crime, we identified Internet facilitated child sexual exploitation as one of our main priorities. Despite the many positive aspects of the Internet for children, it has had a significant negative impact on some child victims of sexual abuse. We agree with the federal government that more needs to be done to identify and rescue children from ongoing sexual abuse and to prosecute those responsible for exploiting them.

The ability of police to identify and rescue children and to prosecute predators is essential. Many Internet Service Providers (ISPs) do cooperate with requests for information when police provide a letter of request. But according to the RCMP's

National Child Exploitation Coordination Centre, 30-40% of requests are denied. That means many predators go undetected, and many children are potentially left in abusive situations.

THE IMPACT OF INTERNET FACILITATED CHILD SEXUAL ABUSE

There are over 1 million child sexual abuse images on the Internet. Twenty thousand new pictures are added every week.[1] There are over 100,000 searches daily. There are tens of thousands of websites that promote sex with children.

The children seen in the images are getting younger and the abusers are getting more violent.[2] Over 85% of the children are under 12, many under 9 and almost one in five are under 3.[3] Eighty percent of the images involve penetration and 20% involve torture or bondage.[4]

Eighty percent of the abuse seen online is committed by people the children know.[5] Many of those who access and trade images are also abusers themselves. One study in the US found that 80% of offenders in prison for child pornography-related offences admitted to being abusers.[6]

---

[1] Unless otherwise stated, the statistics are provided by the RCMP's National Child Exploitation Coordination Centre.
[2] OPP Detective Inspector Angie Howe, *Senate Legal and Constitutional Affairs Committee*, Bill C-2, June 22, 2005.
[3] http://www.mg.co.za/articlePage.aspx?articleid=320210&area=/insight/insight__international/
[4] CTV.ca, July 23, 2006.
[5] C-CAICE
[6] Dr. Peter Collins, *Standing Committee on Justice and Human*, Bill C-2, May 3, 2005.

Therapists, law enforcement and victim services have years of experience dealing with child sexual abuse victims, but there is growing recognition that child sexual abuse images and the Internet complicate the impact of the offences, the recovery of victims and the delivery of services. Tink Palmer, a member of *Stop it Now! UK*, asserts that, "...we need a radical reconsideration of current practices, policies and procedures in the light of new technological conduits for abusing children."[7]

She goes on to say, "the additional trauma for a child who knows that their humiliation has been photographed or filmed, and that people around the world may access and witness it in the immediate present and also long into the future, has serious and complex implications for assisting the child's recovery and for the way such crimes are investigated."[8]

End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes' (ECPAT) contends, "Child pornography amplifies and broadcasts the original act of abuse that it depicts. In doing so, it can substantially aggravate the original offence."[9]

One child sexual abuse victims whose photos were put on the Internet said, "Usually, when a kid is hurt and the abuser goes to prison, the abuse is over. But because XXX put

---

[7] Tink Palmer, "Abusive images: The impact on the child," in ECPAT Newsletter, Issue 49 1/January/2005.
[8] Tink Palmer, "Abusive images: The impact on the child," in ECPAT Newsletter, Issue 49 1/January/2005.
[9] John Carr, "Theme Paper on Child Pornography for the 2nd World Congress on Commercial Sexual Exploitation of Children" p.13
http://www.ecpat.net/eng/Ecpat_inter/projects/monitoring/wc2/yokohama_theme_child_pornography.pdf

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."[10]

Another victim said, "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."[11]

The Supreme Court of Canada, in the case of *R. v. John Robin Sharpe*, said,

> "The child is traumatized by being used as a sexual object in the course of making the pornography. The child may be sexually abused and degraded. The trauma and violation of dignity may stay with the child as long as he or she lives...the child must live in the years that follow with the knowledge that the degrading photo or film may still exist, and may at any moment be being watched and enjoyed by someone."[12]

Victims often do not disclose that photos were taken or videos were made, and even when confronted with such discoveries, some victims will refuse to acknowledge that this was done. "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...Anxiety may intensify where a child understands that images of their abuse will continue to be replicated and circulated to an audience that is both nearby and global long into the future."[13]

---

[10] Julian Sher, *One Child at a Time*, 2007
[11] Julian Sher, *One Child at a Time*, 2007
[12] R. v. Sharpe, [2001] 1 S.C.R. 45, 2001 SCC 2, paragraph 92.
[13] ECPAT International, "Violence Against Children in Cyberspace," 2005. p.41

Children may have difficulties accepting that they cannot control their images; that once they are on the Internet, men around the world may be using them for their own sexual gratification or to groom other children. They must learn to live with the reality that their photos will be on the net and in people's computers forever. ECPAT says,

> "...even where it has been possible to identify a victim, the chances of being able to help the child to recover from the trauma of the initial involvement in the abuse can be seriously compromised if the child learns or comes to believe that images of them engaged in the abusive behaviour might have been scanned, or converted into a digital format in some other way, for storage on a computer or for transmission between computers e.g. over the Internet. This, in effect, makes the image part of a permanent public record. It could, even randomly, suddenly appear on the screen of their next-door neighbour or classmates."[14]

FEDERAL GOVERNMENT'S COMMITMENT TO CHILDREN

There can be little doubt that this Government has repeatedly displayed its commitment to protect children from those who would prey on them. Bill C-22, which would raise the age of consent from 14 to 16, is but one example.

That commitment was also evident in the 2007 Budget, when the Minister of Finance gave an additional $6 million to the RCMP to protect children from sexual exploitation. Minister Flaherty said, "The funding will ensure that those who commit these heinous offences are brought to justice..."

In 2003, the Government of Canada signed the *Canadian Basic Statement of Principles for Victims of Crime*, which commits the federal government to consider and respect the

---

[14] John Carr, "Theme Paper on Child Pornography for the 2nd World Congress on Commercial Sexual Exploitation of Children" p.14
http://www.ecpat.net/eng/Ecpat_inter/projects/monitoring/wc2/yokohama_theme_child_pornography.pdf

privacy of victims to the greatest extent possible; to minimize inconvenience to victims and to take appropriate measures to protect victims. Canada is also a signatory to several key UN declarations that speak to the need to protect and promote the safety and privacy of victims and children.

More recently, Canada with other G8 Ministers agreed to accelerate efforts to combat child sexual exploitation. The G-8 Ministers committed, "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."[15] The Ministers also acknowledged and recognized that the private sector, including Internet Service Providers (ISPs), have a role to play in protecting the world's children." The Ministers recognized that, "Child pornography grievously harms all children: it harms the child who is sexually assaulted in the making of the image; the same child is re-victimized every time that image is viewed."[16]

THE LAWFUL ACCESS DEBATE

For years, the law enforcement community has been calling upon the federal government to reform the *Criminal Code* to enable them to apply real world police tools to the virtual world. For example, police can get a customer's name from a telephone company, but not from an Internet Service Provider (ISP). After a series of consultations, the former government introduced Bill C-74, which among other things (that will not be discussed

---

[15] G-8 Justice and Home Affairs Ministers, May 24, 2007. www.g8.gc.ca/childpornography-en.asp
[16] G-8 Justice and Home Affairs Ministers, May 24, 2007. www.g8.gc.ca/childpornography-en.asp

here in any detail) enhanced law enforcement's capability to access customer name and address (CNA) information from ISPs. Although the bill had problems,[17] it was seen as a welcome initiative by those concerned with law enforcement and the protection of children from Internet sexual predators. Bill C-74 died on the Order Paper when the election was called.

Subsection 7(3)(c) of the *Personal Information Protection and Electronic Documents Act (PIPEDA)* sets out provisions where an organization **may** disclose personal information without consent. It refers 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.

Parliament clearly intended to facilitate the enforcement of criminal law, but the Committee heard that law enforcement has found it to be a hindrance. Of particular concern is with respect to investigations of suspected Internet facilitated child sexual exploitation. Some ISPs do cooperate with law enforcement requests in child sexual abuse investigations, in part because they recognize the uniqueness of the child pornography[18] provisions in the *Criminal Code* - that it is a crime to simply access and view child sexual abuse images. That makes it somewhat different than other crimes. For

---

[17] For example, the bill allowed companies exceptions if it was cost prohibitive. This is not consistent with other industries. Government does not allow the car industry to only take safety measures if they can afford it. When municipalities impose smoking bans on restaurants and establishments, there are no exceptions for establishments that might suffer a financial hardship.

[18] Generally, we prefer to use the term child sexual abuse images (CSAI) rather than child pornography because CSAI is more reflective of what it is we are talking about – permanent records of child abuse. We a woman is raped, we do not call it adult pornography. We should not do it when it comes to children.

example, it is not illegal simply to read hate literature. Unfortunately, not all ISPs cooperate with law enforcement.

The Standing Committee on the Access to Information, Privacy and Ethics conducted a widespread review of the *Personal Information Protection and Electronic Documents Act (PIPEDA)* during the last year. It released its Fourth Report earlier this year.

Mr. Clayton Pecknold of the Canadian Association of Chiefs of Police testified before the Committee and explained the challenges the police currently 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). (February 13, 2007)

On August 16, 2007, I wrote to the Honourable Jim Prentice, Minister of Industry, in relation to *Recommendation #12* of the Committee's Report, which is relevant to this consultation as it reflects the will of the committee and was a unanimous recommendation, indicating support for the recommendation from all parties. The recommendation states,

> *"The Committee recommends 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 [...]"*

The Committee agreed that it is not realistic or necessary to expect police to seek a warrant in these situations. By including subsection 7(3)(c.1), Parliament clearly did not intend for law enforcement to secure a warrant for information that is not considered personal.

IS CNA PERSONAL INFORMATION?

Recently, the Federal Court ruled that EBay had to give personal information about high volume sellers' clients to the Canada Revenue Agency in order to ensure that those individuals are paying the appropriate taxes.[19]

Courts have said that people do not have a reasonable expectation of privacy attributed to their name and address. In *R v. Plant,*[20] 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 thc 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."[21]

The Court of Queen's Bench of Alberta said, "thcrc is no reasonable expectation of privacy with respect to: 1. General banking information - see *R.* v. *Lillico* (1994), 92

---

[19] Paul Waldie, Taxman goes browsing on eBay, Globe and Mail, September 27, 2007
[20] *R. v. Plant*, [1993] 3 S.C.R. 281. This case dealt with marijuana grow-ops and the police obtained information from the electricity company regarding the owner's electricity use.
[21] R. *v.* Plant, [1993] 3 S.C.R. 281

C.C.C. (3d) 90 (Ont. Gen Div.); [1999] O.J. No. 95 (Ont. C.A.); 2. Cellular telephone records - see *R.* v. *Brown,* [2000] O.J. No. 1177 (Sup. Ct. Jus.) at para.63."[22]

In *R. v. Quinn,* in which police requested "tombstone" information regarding several accounts in which cheques had been deposited, the BC Court of Appeal said, "there was no search, much less any unreasonable search as envisioned in the *Charter.*"[23]

If EBay has to give the Canada Revenue Agency the names and addresses of citizens to make sure that taxes are paid, does it not seem strange that Internet Service Providers (ISP) do not have to give the same information to the police trying to find a sexual predator who may be abusing a child? Measures to prevent a predator from abusing a child should be given the same priority as collecting unpaid taxes.

This is not a privacy issue. It is a public safety issue. It is a child safety issue.

Some have suggested that police should be required to get a warrant for this information. This is inconsistent with the view of the courts which have said this kind of information is not personal. This is, after all, information that can be found with a license plate, phone book or driver's license. The reality of Internet facilitated child exploitation investigations is that children may be at immediate risk. Most abusers seen in online abuse images know the child; many are related; and therefore they have ongoing access to the child.

---

[22] *R. v. Haskell*, 2004 ABQB 474
[23] *R. v. Quinn* 2006 BCCA 255 paragraph 93

In 2004, Michael Briere murdered 10 year old Holly Jones minutes after looking at child sexual abuse images online. He walked out of his home and saw the young girl walking down the street. He grabbed her, took her into his home where he sexually assaulted her before killing her and taking steps to dispose of her remains. At his sentencing hearing, Briere told the court he was consumed by desire after viewing child pornography.[24] While this is an extreme example of what can happen, it should be an important reminder to all of us. Law enforcement officers are increasingly seeing children being abused live on the Internet. And none of us know what happens when the predator turns the computer off. He might not do what Michael Briere did, but it is not a leap of logic to suggest a child might be at risk of further abuse.

It is not acceptable to demand law enforcement to waste their valuable time and resources, not to mention the court's time and resources, to get a warrant for information that the Canada Revenue Agency can demand from EBay. This is information they can demand of someone they see jaywalking or through the license plate of someone seen driving away from a car accident. Preventing child sexual abuse and tracking abusers is as important as preventing traffic accidents and enforcing street laws.

The suggestion that law enforcement secure a warrant for CNA assumes law enforcement can get a warrant in these circumstances, which may not be the case. It is not a question of inconvenience or making a police officer's job easier; it is about rescuing children.

---

[24] CBC News Online, http://www.cbc.ca/news/background/jones_holly/

The government's Consultation Paper says, "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.*"

The good news is that many ISPs are cooperating with police without a warrant, although it remains to be seen what the impact of the Minister's recent comments will be on those companies.

The bad news is requests are denied 30 to 40% of the time.[25] That means 30% of investigations might end on the starting block, and children at risk are left in those abusive situations. Even if the number was lower, it still would not be acceptable. It is unacceptable that we leave a child in an abusive situation one day longer than necessary. Those children must not be sacrificed for the misplaced concern for individual privacy.

The recent debate has created the perception that police want more than just CNA; that they want access to emails. It has also left people with the mistaken belief that police can easily get a warrant in these circumstances. The reality is quite different.

This is what law enforcement refer to as the pre-warrant stage. It is the beginning of an investigation and they need a name to begin the investigation. If they get a name and find out, for example, that John Doe has a 5 year old girl who matches the description of the

[25] RCMP's National Child Exploitation Coordination Centre

images they found online, then they might knock on John's door and save that little girl from being raped that night. But if they cannot get John Doe's name and address, they will not rescue that child.

It is important to note that getting CNA does not mean that the customer is the perpetrator. It does not place him/her in front of the computer at the time the images were traded (for example). An investigation will be required to determine that. But again, it begins with a name and address.

Other countries, including the UK, Australia and the US, do not require law enforcement to secure a warrant before accessing CNA from an ISP. In fact, the scheme set out in Bill C-74 appeared to be more restrictive than that of the other three countries."[26]

WHAT ABOUT THE PRIVACY OF THE CHILD?

At the risk of being repetitive, this is not a privacy issue but a child safety issue. It is unfortunate, given that the debate has focused so much on privacy, that not one word has been spoken about the privacy interests of the children whose images are being traded like baseball cards. The *Canadian Statement of Basic Principles of Justice for Victims of Crime* requires the federal government to consider the privacy interests of victims.

---

[26] Dominique Valiquet, Telecommunications and Lawful Access: II. The Legislative Situation in the United States, the United Kingdom and Australia, 28 February 2006, Library of Parliament, http://www.parl.gc.ca/information/library/PRBpubs/prb0566-e.html.

The Supreme Court said,

> "Child pornography also undermines children's right to life, liberty and security of the person as guaranteed by s.7....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."[27]

Is there any more serious privacy violation than to allow images of a child being raped to be distributed to hundreds of thousands of sexual predators? Imagine growing up knowing those photos are available forever, for anyone to see, and you have no control over them. It should put the controversy over releasing a name in perspective.

CONCLUSION

This debate is not about increasing police powers or the Government's ability to monitor people's activity on the web. It is about rescuing children from potentially abusive situations and prosecuting those who might be abusing and exploiting them.

Everyday, police officers across the country sit in front of computers and sift through tens of thousands of images and watch videos of the most horrific abuse imaginable. They hear the screams of pain. They see the tears.

---

[27] R. v. Sharpe, [2001] 1 S.C.R. 45, 2001 SCC 2, paragraph 189.

If society is going to ask them to do this work, they need to give them the tools to finish the job. Not for the police, not to make their job easier, but for the children.

During a presentation at the NCECC/OPP recent conference, a short audio clip of a little girl being raped by her father.[28] She said, "Daddy, it hurts. It hurts so bad."

What if police needed CNA to help find her but the ISP said no and they could not get a warrant? It is unspeakable that a father would do that to his child, but it would be unforgivable if he was allowed to do it again.

[28] The presenter was illustrating how new software can be used to enhance sound.

RECOMMENDATIONS:

As Federal Ombudsman for Victims of Crime, I recommend the federal government enact legislation requiring ISPs to provide CNA information to law enforcement investigating Internet facilitated child sexual abuse cases. Legislation is necessary to clarify that a judicial authorization is not necessary and that the current practice in which many ISPs accept written requests for CNA from authorized law enforcement officers investigating Internet facilitated child sexual abuse be adopted.

Furthermore, in addition to audit results being provided to the Privacy Commissioner (as was proposed in the consultation document), I recommend that audit results also be provided to the Federal Ombudsman for Victims of Crime.

Public Safety Canada | Sécurité publique Canada

Deputy Minister | Sous-ministre

Ottawa, Canada
K1A 0P8

SECRET

FEB 1 5 2008

6950-13 / 350587

MEMORANDUM FOR THE MINISTER

SUMMARY OF INPUT RECEIVED FROM THE CONSULTATION ON ACCESS TO CUSTOMER NAME AND ADDRESS (CNA) INFORMATION
(For Information and Decision)

ISSUE

- Approval of a summary of participant feedback received in relation to the public consultations on CNA information, and the posting of the summary (**TAB A**), as well as a listing of the groups and individuals who participated in the consultation (**TAB B**), on the departmental website.

BACKGROUND

- Consultations took place from early September to mid-October, 2007. A consultation document was posted on the Public Safety Canada website on September 12, 2007. The public was invited to submit written comments via email or mail, with a deadline of October 12, 2007. Thirty-four written submissions were received from the general public, either through the Public Safety website or through your office.

- Twenty-seven stakeholder groups and individuals, including representatives of law enforcement, victims' groups, privacy stakeholders, and the telecommunications industry, participated through written submissions and/or meetings with departmental officials. Of these, twenty-five consented to having their name or their organization's name posted on the Public Safety website.

- Thank-you letters have been sent to all participants.

CONSIDERATIONS

- The summary has been reviewed by officials from Industry Canada, Justice Canada, the RCMP, CSIS and the Competition Bureau. Representatives of these departments and agencies participated in the meetings with stakeholders and have indicated their support for the document.

- As the summary indicates, there is no consensus on the issue of police and CSIS access to CNA information. Law enforcement considers this access as an essential investigative tool, with privacy concerns being minimal. Victims' groups support on-request access to CNA to prevent crime and victimization, in particular online child sexual exploitation. Industry representatives expressed concerns over cost, competitiveness, client privacy expectations, and the need for clear obligations in law. Privacy advocates do not feel that law enforcement has adequately demonstrated (i.e. through empirical evidence) the need for on-request access to CNA.

Posting on the Public Safety Website

- Given the continued public and media interest in the consultations and the issue of lawful access in general, it is proposed that the summary be posted on the Public Safety Canada website. It is normal practice for the results of public consultations to be made public and doing so may serve to broaden public understanding of the issue. Failing to post the summary may serve to perpetuate the false perception in the media that the Department was attempting to conduct "secret" consultations.

- The names of stakeholders (excluding members of the general public) who participated in the consultations will be made public; however, there will be no attribution to the substance of their participation. Participants were not advised that their written submissions would be posted. It would therefore be inappropriate to do so. It should be noted, however, that some organizations have chosen to post their submissions on their own websites (e.g. the Information Technology Association of Canada, and the Office of the Privacy Commissioner of Canada).

Key Issues and Linkages

- The debate over whether a warrant is always required for agencies to access personal information – which was fairly intense during the period of the consultations - will likely resurface with the posting of a summary.

- There may be questions with respect to the purpose of the consultations. While the media reported that the purpose of the consultations was to "ensure Internet companies are aware of their need to comply when presented with court orders", in fact, the purpose was to provide a range of stakeholders, including the general public, with an opportunity to express their current views and identify any new considerations with respect to the question of access to CNA by law enforcement and CSIS.

- Questions may arise regarding the *Personal Information Protection and Electronic Documents Act* (PIPEDA) Review process, in particular, the question of whether a warrant is needed for companies to provide personal information to law enforcement and other agencies. The Government's formal response to the Review takes the position that PIPEDA does not require a warrant or court order for the disclosure of such information. Public consultation on the Review concluded on January 15, 2008. Not relevant

RECOMMENDATIONS

- It is recommended that you approve the consultation summary document and the list of participants for posting on the departmental website.

- Should you agree, officials will begin development of a communications plan, possibly including a news release and media lines. Once the communications plan has been approved, the consultation summary and list of participants will be immediately posted on the departmental website.

Suzanne Hurtubise

Approved

Not approved

Enclosure: (2)

SUMMARY OF PUBLIC CONSULTATION ON

ACCESS TO CUSTOMER NAME AND ADDRESS INFORMATION

FOR PUBLIC SAFETY PURPOSES

APRIL 2008

INTRODUCTION

Public Safety Canada, in collaboration with Industry Canada, undertook a public consultation on the subject of law enforcement and national security agencies' access to customer name and address information (CNA) in the possession of telecommunications service providers (TSPs) for public safety purposes. CNA information generally refers to basic identifiers such as a name, address, cell phone identifiers, Internet protocol (IP) and email addresses, or similar identifiers. The consultations were initiated in September 2007 and concluded in October 2007.

The purpose of the public consultation was to provide a range of stakeholders and the general public with an opportunity to express their current views and identify any new considerations with respect to this issue. Stakeholders were asked to consider a number of important factors, including: the challenges faced by law enforcement and national security agencies in the face of new technologies; the need to preserve and protect the privacy rights of all Canadians; and maintaining the competitiveness of the telecommunications sector.

A consultation document was posted on the Public Safety Canada website on September 12, 2007. The public was invited to provide input into the consultation process by October 12, 2007. Interested individuals and organizations from across Canada provided written comments by letter or through the Public Safety Canada consultation webpage. In addition, meetings and teleconferences were held with a number of groups and individuals. Those who participated in the consultation included representatives of law enforcement, victims groups, industry, civil liberties organizations, individuals and groups with an interest in privacy issues, and members of the general public.

SUMMARY

This summary is an overview of the comments and written submissions received from all groups and individuals who participated in the consultation process. The views and opinions of participants are presented below within one of five categories: law enforcement, victims groups, industry, privacy advocates, and public submissions. These categories are generally reflective of the orientation of participants, and are used to assist in presenting the views, opinions and information received.

LAW ENFORCEMENT

Law enforcement participants stressed the need for timely and consistent on-request access to CNA information for a variety of policing purposes, including the investigation of serious crimes such as child sexual exploitation, terrorism and other criminal activities. Participants were strongly of the view that legislation requiring the disclosure of CNA to law enforcement was essential for them to perform their duties effectively. Key features of any legislation would include clear obligations for TSPs and consistent practices with regard to the disclosure of CNA.

- Expressed concern over the lack of a clear legal framework governing TSP disclosure of CNA. Without clear obligations in the law, a variety of practices have developed among

TSPs with respect to the release of basic customer information. TSPs are deciding when to release CNA to police, under what circumstances, and with little consistency overall; thereby influencing the degree to which police are able to follow up on a potential lead, pursue an investigation, or rescue a victim from danger. If the TSP is not cooperative when a request for CNA is made, law enforcement agencies may have no means to compel the disclosure of this information.

- Expressed frustration over the increasing reluctance on the part of TSPs to assist police in accessing basic CNA information. This was linked to the area of child sexual abuse and exploitation, and was also flagged as a concern relevant to other investigations (especially on-line) and the pursuit of general policing duties.

- Noted that many TSPs do provide police with CNA information in child sexual abuse investigations, in part because they understand the seriousness of the crime, while also recognizing the unique challenges involved in fighting it. At the same time, according to the RCMP's National Child Exploitation Coordination Centre, on average one-third or about 35 percent of CNA information requests involving child sexual exploitation cases are denied, leaving many predators undetected and many children in abusive situations.

- Supported strong privacy safeguards as an important component of any legislative proposal providing for access to CNA upon request, but they did not consider judicial pre-authorization as an appropriate option (or even feasible in most instances). Emphasized that CNA is "pre-warrant" information that simply provides law enforcement with basic, non-sensitive identification information which carries little or no expectation of privacy. This information is often vital in early stages of investigations, and without which further investigation leading to a warrant may not be possible. Described CNA as telephone book information – with email and IP addresses analogous to traditional telephone identifiers, such as name, telephone and civic address.

- Described CNA information as a tool to investigate a lead and to help to confirm or remove people as potential suspects in a case. Emphasized that an investigation does not end with the acquisition of CNA information. Should law enforcement decide to pursue further investigatory measures that require prior judicial authorization, such as intercepting communications or searching a residence, police would seek an appropriate order from a court.

- Supported the use of administrative safeguards to ensure appropriate access to CNA information (in the context of a legislated obligation to provide the information on request); the safeguards could include limits on who can have access to the information and how it is used, as well as requirements for internal audits. Emphasized that lawful access to CNA does not include content of communications or website activity, and noted that police would clearly continue to obtain the necessary court orders to track web activity or to intercept private communications.

- Spoke to the favourable working relationships they have built over the years with established TSPs, for example the major phone companies, in requesting CNA in the course of their

duties. At the same time, pointed to the practical difficulties and burdens in trying to work with the over 400 Internet service providers (ISPs) that currently operate in the Canadian market.

- Expressed concern over the extremely high resource demands that would be placed on law enforcement organizations and the courts if police were required to seek judicial pre-authorization for all CNA inquiries.

- Noted that no law prohibits ISPs from informing a customer of police interest in their CNA information, and the related risk that ongoing criminal investigations can be compromised if such information is provided to the customer. Advised that some ISPs openly advertise their lack of cooperation with police to attract customers and hinder criminal investigations by informing customers that they will delete an account in the event of a "personal emergency".

- Emphasized that other countries, including the United Kingdom, Australia and the United States, do not require their law enforcement agencies to secure judicial pre-authorization to obtain CNA from a TSP, and that administrative safeguards appear to work well in those jurisdictions.

VICTIMS GROUPS

Victims groups shared many of the concerns and views expressed by law enforcement representatives. They strongly emphasized that access to CNA is first and foremost a public safety issue, and that the individual privacy rights of those who may be the subject of a criminal investigation do not, and should not, override the privacy rights of victims of crime - keeping in mind many victims are children who need to have police investigate crimes against them in order to protect their privacy (for example, where images of abuse are being displayed on the Internet). They highlighted that CNA is often crucial in the ability of law enforcement to rescue children from abusive situations and prosecute those responsible.

- Emphasized the difficulty for law enforcement in investigating child pornography and child luring cases without access to basic Internet identifiers such as IP and email addresses, noting that anonymity is inherent in many online communications.

- Expressed frustration over the lack of cooperation on the part of some TSPs to assist police by providing access to basic CNA information. Acute concern was expressed in the area of Internet-facilitated child sexual exploitation, while recognizing that CNA information may be important in other contexts as well.

- Victims groups shared the view of law enforcement that CNA was "pre-warrant" information that should not be subject to judicial pre-authorization. Stressed that the scope of CNA information accessible upon request should be well defined and recognized the need for strong safeguards to protect against possible abuses and ensure public confidence.

- Argued that TSPs have a responsibility for the environment that they create and profit from, and that part of that responsibility is to respond to law enforcement requests for assistance in

accessing CNA for public safety purposes. Expressed concerns that police are forced to rely on moral suasion, calls to abide by civic duty, and the goodwill of TSPs, when the lives of children and other victims hang in the balance.

- Noted that the Government of Canada signed the *Canadian Basic Statement of Principles for Victims of Crime* in 2003, which commits the federal, provincial and territorial governments to consider and respect the privacy of victims to the greatest extent possible and to take measures to protect victims. Noted that G-8 Ministers committed to ensuring the implementation and effectiveness of laws relating to child pornography.

- Recommended that the results of any audits of practices that might be required by new legislation should be provided to the Federal Ombudsman for Victims of Crime.

INDUSTRY

Industry - comprising telecommunications industry associations, individual TSPs, and other organizations with an interest in telecommunications - generally supported law enforcement and national security agencies' (LEAs) access to CNA for public safety purposes in appropriate circumstances. The main preoccupations for industry, should any new legislation come into place, were: to have clear and reasonable obligations in law; that companies receive reasonable compensation for costs incurred in providing CNA information; and, concern that new information collection, retention or verification obligations would not be created.

- Held that any new legislation or regulations must clearly outline TSP obligations, recognizing that many customers expect information to be protected and not disclosed. Rather than relying on discretion or judgement calls, they indicated a desire to see specifics regarding when, under what circumstances, and to whom to release CNA.

- If new legislation were to require on-request access to CNA by police and the Canadian Security and Intelligence Service (CSIS), strong administrative safeguards would be essential to protect the privacy interests of their customers. General acknowledgment that the privacy rights of individuals must be balanced with the requirements of law enforcement officials to track and prosecute criminals. Potential safeguards listed in the consultation document were seen as generally reasonable and rigorous.

- Some TSPs expressed a preference to continue to provide CNA only subject to a warrant or in exigent circumstances (i.e. imminent threat of harm to person or property). Where exigent circumstances or urgent need is demonstrated, many noted that they respond to LEAs as quickly and as diligently as possible. A number said that more clarity was needed to define the scope of exigent circumstances and when information must be provided.

- Some suggested it would be advantageous to look into alternative models, such as an expedited judicial authorization process (warrant or production order), or the creation of a lower threshold warrant for accessing CNA.

- Indicated that the scope of the CNA information listed in the consultation document extended beyond what might be commonly regarded by the general public as "basic customer information" (i.e. cell phone and Internet identifiers). Suggested that the types of "basic identifiers" sought for wireless and Internet services are more onerous to produce than those of traditional telecommunications services due to the sophistication of the technologies employed. As such, wireless and Internet providers felt they should not be compelled to provide greater levels of information than other TSPs operating traditional telecommunications technologies.

- Noted that traditional "tombstone data" such as customer name, civic address and telephone number information may be less privacy-sensitive than other types of identifiers. Underlined the importance of having customers understand there is a legal framework within which this information is provided to police.

- Recommended important safeguards with regard to designated officers, including a process in place to limit the number of contact points, ensure consistency, and validate the authority of the LEA officials requesting CNA. Some also suggested working with LEAs to create a standardized CNA request form to facilitate any request process.

- Suggested that provisions in any new legislation may need to deal differently with smaller and larger TSPs. New measures could have greater impacts and relative resource implications for smaller TSPs (e.g., any increase in requests for CNA may necessitate hiring and training more personnel, as well as upgrading or automating information systems).

- Expressed concern that the volume of requests for CNA could increase substantially under any new legislation if there were no judicial pre-authorization, with a corresponding and likely substantial increase in costs to TSPs.

- Noted that Canada's telecommunications industry has a long history of working cooperatively with law enforcement. Acknowledged that the ability to obtain CNA is an important tool for LEAs in their efforts to protect society, and underscored a desire to continue their positive relationships with law enforcement.

- Noted that large TSPs maintain dedicated security departments whose sole purpose is to respond to law enforcement requests and comply with court orders; that these services are provided in the interest of public safety by TSPs; and that there is an associated cost to providing this assistance, which is not insignificant.

PRIVACY ADVOCATES

Privacy stakeholders generally recognized that a lack of consistency with regard to CNA disclosure practices by TSPs represents a hindrance to law enforcement in their ability to pursue leads and investigate crimes. This lack of consistency alone, however, is not a sufficient justification for warrantless access to CNA, which most consider infringes upon civil liberties and individual privacy. The need for access to information must be demonstrated and concern was expressed that evidence to date is lacking. Above all, they stressed the importance of

appropriate oversight in the CNA disclosure process, with a very strong preference for judicial pre-authorization, to protect privacy and other rights under the *Canadian Charter of Rights and Freedoms*.

- Indicated that the law enforcement community should first clearly demonstrate the need for CNA, before the creation of a requirement for TSPs to provide this information on-request, is considered. Expressed the opinion that in the majority of cases police can obtain the information they need through traditional investigative means, including the use of a warrant or production order.

- The majority expressed that judicial pre-authorization should always be required for the release of any personal information to LEAs. Several suggested that the necessity for judicial pre-authorization may depend on the nature of the information being sought (e.g. warrants may not be necessary for information already in the public domain or for "tombstone data" including name, address, and telephone numbers). Some believed that options for access to CNA without judicial pre-authorization may be reasonable; however, most took the view that LEAs needed to do more to publicly demonstrate why there is a need to obtain it without judicial pre-authorization.

- Some contended that existing provisions within the *Criminal Code* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) provide the police with an adequate legislative framework and powers to investigate crimes, including Internet-related crime. They suggested that what is needed is more education and an effort to foster an enhanced cooperative working environment between TSPs and law enforcement.

- Some suggested examining mechanisms in the *Criminal Code* that either enable access to certain information at lower thresholds (i.e. the creation of a lower threshold warrant), or through the use of an expedited process for judicial authorization. Others felt that lowering the judicial threshold would be inappropriate given that personal information is involved. Opposition was also expressed by some to the idea of expediting CNA authorizations, suggesting that the *Criminal Code* already provides for an expedited process in which LEAs can access CNA in urgent situations – i.e. s.487.11 provides for warrantless searches in cases of exigent circumstances, including an urgent threat of serious harm to any person or property.

- Some felt that without judicial pre-authorization, the purposes for which law enforcement may demand CNA must be narrowly and precisely circumscribed (e.g. through a prescribed list of circumstances under which LEAs could obtain access to CNA upon request). Evidence would be required to justify the listing of circumstances in which warrantless, on-demand access to CNA would be appropriate.

- Shared industry's concern that the scope of the information listed in the consultation document extended beyond what might be appropriately regarded by members of the public as "basic customer information" (i.e. cell phone and Internet identifiers).

- Argued that although CNA pertains to seemingly innocuous personal identifiers, it has the potential to reveal sensitive personal information when combined with other information. For instance, separate pieces of information about an individual could potentially be combined so as to reveal more intimate personal information.

- Stressed the need for strong legislative safeguards to ensure the appropriate access to, use, and handling of CNA by LEAs. Concerned about the potential for abuse, such as the pursuit of "fishing expeditions" or the potential for LEAs to accumulate and retain large amounts of personal information on individuals. Pointed to the recent reported abuses and irregularities in the United States involving the use of administratively authorized search procedures. Some contributors suggested that the safeguards in the consultation document were insufficient in any context, and that additional safeguards should be in place even where judicial authorization is obtained.

- Indicated that a continuing review of any administrative model that might be created by statute (i.e., on-request access, with administrative safeguards) would be imperative. There would be a need to ensure that changes in technology and/or industry practices do not result in a process that violates the *Canadian Charter of Rights and Freedoms* by unduly infringing upon individuals' expectations of privacy.

- One participant suggested the creation of a working group in statute that would comprise government, industry, privacy and civil society representatives to provide ongoing advice on the administration of any legislation and review practices.

PUBLIC SUBMISSIONS

The majority of public submissions were opposed to law enforcement access to CNA information without judicial pre-authorization. Some mistakenly believed that judicial pre-authorization is required today in all cases. A perception was expressed by some that law enforcement may be attempting to extend its reach too far into the private lives of Canadians.

- Expressed strong opposition to law enforcement access to information in the online context. Many were mistakenly of the view that law enforcement and national security agencies were seeking unwarranted access to the content of communications, including email content and websites visited.

- Suggested that an absence of judicial pre-authorization creates the potential for abuses to occur through unnecessary access to personal information. Comparisons were made with recent reported abuses and irregularities in the United States.

- Expressed the view that there is a lack of publicly available evidence clearly demonstrating law enforcements' need to access CNA without judicial pre-authorization.

RÉSUMÉ DE LA CONSULTATION PUBLIQUE AU SUJET DE L'ACCÈS AUX RENSEIGNEMENTS RELATIFS AU NOM ET À L'ADRESSE DES CLIENTS À DES FINS DE SÉCURITÉ PUBLIQUE

AVRIL 2008

INTRODUCTION

Sécurité publique Canada, en collaboration avec Industrie Canada, a entrepris une consultation publique au sujet de l'accès par les organismes d'application de la loi et de sécurité nationale, aux renseignements relatifs aux noms et aux adresses des clients (NAC), en la possession des fournisseurs de services de télécommunication (FST) aux fins de la sécurité publique. Les renseignements relatifs aux NAC concernent généralement des identificateurs de base tels qu'un nom, une adresse, des identificateurs de téléphone cellulaire, des adresses IP et de courrier électronique, ou d'autres identificateurs similaires. La consultation a débuté en septembre 2007 et s'est terminée en octobre 2007.

La consultation visait donner à toute une gamme d'intervenants et au public l'occasion de donner leurs points de vues et de cerner tous les nouveaux éléments à considérer relativement à cette question. Les intervenants devaient tenir compte d'un certain nombre de facteurs importants, notamment, les difficultés auxquelles font face les organismes d'application de la loi et de sécurité nationale devant les nouvelles technologies, la nécessité de maintenir et de protéger le droit à la vie privée de tous les Canadiens et toutes les Canadiennes et la nécessité d'assurer la compétitivité du secteur des télécommunications.

Un document aux fins de la consultation a été affiché sur le site Web de Sécurité publique Canada le 12 septembre 2007. Le public a été invité à faire parvenir ses observations avant le 12 octobre 2007. Les particuliers et les organismes concernés dans l'ensemble du Canada ont fait parvenir leurs commentaires écrits, par courrier ou sur la page Web de consultation de Sécurité publique Canada. De plus, un certain nombre de rencontres et de téléconférences ont eu lieu avec des groupes ou des particuliers précis. Des représentants des forces de l'ordre, de groupes pour victimes, de l'industrie et d'organismes de défense des droits civils, ainsi que des personnes et des groupes intéressés au droit à la vie privée et le grand public ont participé à la consultation.

RÉSUMÉ

Le présent résumé donne un aperçu des observations orales et écrites présentées par les différents groupes ou particuliers ayant participé au processus de consultation. Les points de vue et les avis des participants sont présentés ci-dessous dans l'une des cinq catégories suivantes : l'application de la loi, les groupes pour victimes, l'industrie, les défenseurs du droit à la vie privée, et le public. Ces catégories représentent de façon générale l'orientation des participants et facilitent la présentation des points de vie, des avis et de l'information reçus.

APPLICATION DE LA LOI

Les participants du secteur de l'application de la loi ont insisté sur la nécessité d'accéder en temps opportun et de façon uniforme aux NAC à des fins policières diverses, notamment dans le cadre d'enquêtes relatives à des crimes graves, comme l'exploitation sexuelle des enfants, le terrorisme et d'autres activités criminelles. Les participants étaient convaincus de la nécessité d'établir des dispositions législatives obligeant la divulgation des NAC aux organismes

d'application de la loi, estimant que l'accès à cette information était essentiel à l'exercice de leurs fonctions. Selon eux, les grandes caractéristiques de toutes mesures législatives quelles qu'elles soient devraient inclure des obligations claires pour les FST et des pratiques uniformes en ce qui concerne la divulgation des NAC.

- Les participants ont exprimé des préoccupations au sujet de l'absence d'un cadre juridique clair régissant la divulgation par les FST des NAC. En l'absence d'obligations claires contenues dans les dispositions législatives, des pratiques très variées se sont développées parmi les divers FST en matière de communication de renseignements de base sur les clients. Les FST décident du moment où ils communiquent les NAC aux policiers et des circonstances où ils le font, et leurs pratiques individuelles sont très peu uniformes, de sorte qu'ils ont une influence sur le degré auquel les services de police peuvent suivre la trace d'un indice potentiel, poursuivre leur enquête ou se porter au secours d'une victime. Si les FST ne se montrent pas coopératifs à l'égard d'une demande de NAC, les organismes d'application de la loi (OAL) n'ont aucun moyen de les forcer à divulguer cette information.

- Les participants ont exprimé leur frustration en raison du fait que les FST hésitent de plus en plus à aider les services de police à accéder aux NAC. Le problème se pose en ce qui a trait aux cas d'abus et d'exploitation sexuelle des enfants, mais aussi dans le cadre d'autres enquêtes (en ligne surtout), de même que dans le cadre d'activités policières de nature générale.

- Les participants ont mentionné qu'un grand nombre de FST communiquent les NAC dans le cadre d'enquêtes sur l'exploitation sexuelle des enfants, en partie parce qu'ils sont conscients de la gravité du crime, mais aussi parce qu'ils reconnaissent les difficultés particulières inhérentes à la lutte contre ce type d'activités. Malgré tout, selon le Centre national de coordination contre l'exploitation des enfants (CNCEE), en moyenne environ le tiers ou 35 p. 100 des demandes d'accès aux NAC relatives à des affaires d'exploitation sexuelle des enfants sont refusées, faisant en sorte qu'un grand nombre de prédateurs ne sont pas détectés et que bien des enfants ne peuvent être sauvés de situations d'abus.

- Les participants ont exprimé leur soutien à l'existence de mesures rigoureuses de protection du droit à la vie privée comme élément important de toute proposition législative permettant l'accès sur demande aux NAC, mais ils estiment toutefois pas qu'il n'est pas approprié (ou même possible dans la plupart des cas) d'exiger une autorisation judiciaire préalable. Ils ont insisté sur le fait que les NAC constituent seulement une information de base de nature non délicate, pour laquelle il y a peu ou pas d'attentes en matière de vie privée et qu'il s'agit en fait d'information préalable à l'obtention d'un mandat. Or, ces renseignements sont souvent essentiels en début d'enquête, car il est parfois impossible sans ceux-ci de poursuivre l'enquête et d'obtenir un mandat. Les participants ont décrit les NAC comme des renseignements que l'on trouve dans l'annuaire téléphonique, assimilant l'adresse électronique et l'adresse IP aux identificateurs téléphoniques, tels que le nom, le numéro de téléphone et l'adresse municipale.

- Ils ont indiqué que les NAC sont un outil qui leur permet de suivre une piste ou de confirmer ou d'éliminer un éventuel suspect. Ils ont attiré l'attention sur le fait que l'enquête ne se

termine pas avec l'obtention des NAC. Si les représentants des forces de l'ordre décident de prendre pour leur enquête d'autres mesures, qui exigent une autorisation judiciaire préalable, comme l'interception de communications ou la fouille d'une résidence, la police demandera un mandat à la cour.

- Les participants acceptent l'utilisation de mesures administratives de protection afin d'assurer un accès légitime aux NAC (si la loi oblige les FST à fournir cette information sur demande); ces mesures de protection pourraient limiter les personnes pouvant accéder à ces renseignements et les fins auxquelles ceux-ci peuvent être utilisés, et pourraient exiger la tenue d'enquêtes internes. On pourrait aussi exiger la tenue de vérifications internes. Les participants ont souligné que l'accès légal aux NAC ne comprend pas l'accès au contenu des communications ou des activités sur un site Web, et ils ont souligné que la police serait toujours tenue d'obtenir les mandats nécessaires auprès des tribunaux, pour suivre les activités sur le Web ou pour intercepter des communications privées.

- Les participants ont mentionné les relations de travail positives qu'ils ont nouées au fil des ans avec les FST, par exemple, les sociétés du domaine de la téléphonie, lorsqu'ils demandent des NAC dans le cadre de leurs fonctions. Parallèlement, ils ont mentionné les difficultés et le fardeau dans la pratique que représente le fait de travailler avec plus de 400 fournisseurs de services Internet (FSI) qui sont actuellement sur le marché canadien.

- Ils ont exprimé leurs inquiétudes quant aux contraintes très élevées que subiront les OAL et les tribunaux si l'on exige l'obtention d'une autorisation judiciaire préalable chaque fois que l'on veut obtenir les NAC.

- Ils ont signalé que, à l'heure actuelle, aucune loi n'interdit aux FSI d'informer un client que la police cherche à obtenir leurs NAC, ce qui peut compromettre des enquêtes criminelles en cours si cette information est divulguée au client. Ils ont indiqué que certains FSI , pour attirer des clients, font ouvertement connaître le fait qu'ils ne collaborent pas avec la police, et nuisent aux enquêtes criminelles en disant aux clients qu'ils supprimeront tout compte en cas d'« urgence personnelle ».

- Les participants ont fait valoir que dans d'autres pays, y compris le Royaume-Uni, l'Australie et les États-Unis, les OAL ne sont pas obligés de demander une autorisation judiciaire pour obtenir les NAC, de la part des FST, et que les mesures administratives de protection mises en place dans ces pays semblent bien fonctionner.

<u>GROUPES POUR VICTIMES</u>

Les groupes pour victimes partageaient en grande partie les préoccupations et les points de vue des représentants des forces de l'ordre. Ils ont beaucoup insisté sur le fait que l'accès aux NAC est d'abord et avant tout une question de sécurité publique, et que le droit à la vie privée des particuliers qui pourraient faire l'objet d'une enquête criminelle ne doit pas avoir préséance sur les droits des victimes d'actes criminels, compte tenu du fait que de nombreuses victimes sont des enfants, qui ont besoin que la police enquête sur des crimes commis contre eux pour protéger leur vie privée (par exemple, lorsque des images d'agressions sont affichées sur Internet). Ils ont

fait valoir que les NAC jouent souvent un rôle déterminant, puisqu'ils permettent aux OAL de sauver des enfants de situations d'abus et de poursuivre les responsables.

- Les participants ont mis en relief le fait qu'il est difficile pour les organismes d'application de la loi d'enquêter sur des affaires de pornographie juvénile et la cyberprédation, en l'absence d'identificateurs Internet de base, comme l'adresse IP ou électronique, rappelant que l'anonymat est très souvent un caractère inhérent des communications en ligne.

- Ils ont exprimé leur frustration à l'égard du manque de coopération de certains FST, qui refusent d'aider la police à accéder aux NAC. Ils étaient particulièrement inquiets de ce problème dans le contexte de l'exploitation sexuelle des enfants sur Internet, mais étaient conscients que l'accès aux NAC était aussi important dans d'autres contextes.

- Les groupes pour victimes considèrent, comme les organismes d'application de la loi, les NAC comme des renseignements préalables à l'obtention d'un mandat et pour lesquels il ne devrait pas être nécessaire d'obtenir une autorisation judiciaire préalable. Ils ont souligné qu'il importera de bien définir les renseignements qui devront être communiqués sur demande, et sont conscients de la nécessité de mettre en place des mesures de protection vigoureuses, afin d'éviter les abus et de maintenir la confiance du public.

- Ils ont soutenu que les FST ont une responsabilité à l'égard de l'environnement qu'ils créent et dont ils tirent profit, notamment celle de donner suite aux demandes présentées par les organismes d'application de la loi pour obtenir l'accès aux NAC à des fins de sécurité publique. Ils se sont dits préoccupés par le fait que les services de police doivent recourir à la persuasion morale, insister sur le devoir civique ou encore faire appel à la bonne volonté des FST, lorsque la vie d'enfants et d'autres victimes en dépend.

- Ils ont mentionné que le gouvernement du Canada avait signé la *Déclaration canadienne des principes fondamentaux de justice relatifs aux victimes de la criminalité* en 2003, dans le cadre duquel il s'est engagé à tenir compte des impératifs de la vie privée des victimes et les respecter autant que possible, et à prendre les mesures pour protéger les victimes. Ils ont également observé que les ministres du G-8 se sont engagés à mettre en œuvre des lois pour lutter contre la pornographie juvénile, et à assurer la portée réelle de ces lois.

- Les participants ont recommandé que l'on communique les résultats des vérifications des pratiques requises par une nouvelle loi, à l'ombudsman fédéral des victimes d'actes criminels.

INDUSTRIE

L'industrie, c.-à-d., les associations de l'industrie des télécommunications, les FST et d'autres organismes concernés, appuie de façon générale le principe de l'accès, dans des circonstances appropriées, par les organismes d'application de la loi et de sécurité nationale aux NAC, à des fins de sécurité publique. L'industrie a soulevé quelques grandes préoccupations quant à la mise en place de nouvelles mesures législatives : elle souhaite que les obligations soient raisonnables et clairement définies, que les entreprises soient dédommagées pour les coûts de la

communication des NAC, et qu'aucune autre obligation ne soit imposée en ce qui concerne la collecte, la conservation et la vérification de renseignements.

- Les participants ont soutenu que toute nouvelle disposition législative ou réglementaire doit définir clairement les obligations des FST, car bon nombre de clients s'attendent à ce que leurs renseignements personnels soient protégés et ne soient pas divulgués. Ils ne veulent pas s'en remettre au jugement ou à la discrétion d'une personne, mais souhaitent plutôt que l'on précise clairement les cas et les circonstances où les FST doivent communiquer les NAC, ainsi que les personnes à qui ils doivent l'être.

- S'il devient nécessaire, par suite de l'adoption de mesures législatives, de fournir sur demande des NAC à la police et au Service canadien du renseignement de sécurité, il sera essentiel de mettre en place de solides mesures administratives pour protéger le droit à la vie privée de leurs clients. Les représentants sont conscients de la nécessité d'établir un équilibre entre le droit à la vie privée et l'obligation pour les organismes d'application de la loi de surveiller et de poursuivre les criminels. Ils estimaient raisonnables et rigoureuses les mesures proposées dans le document de consultation.

- Certains FST préféreraient continuer à communiquer les NAC seulement sur présentation d'un mandat ou en cas d'urgence (p. ex., menace imminente visant une personne ou des biens). Lorsque les circonstances l'exigent ou qu'il s'agit d'une urgence, un grand nombre de FST ont indiqué qu'ils communiquaient rapidement et avec diligence les NAC. Un certain nombre de répondants ont indiqué qu'il faudrait définir plus clairement ce que l'on entend par situation d'urgence, et quand l'information doit être fournie.

- Certains ont suggéré qu'il serait sans doute avantageux d'examiner des solutions de rechange, telles que la mise en place d'un processus accéléré d'autorisation judiciaire (mandat ou ordonnance de production) ou encore l'établissement de critères moins rigoureux pour la délivrance de mandats pour l'accès aux NAC.

- Ils ont également signalé que les renseignements énumérés dans le document de consultation ne se limitent pas à ce que les membres du public considèrent habituellement comme des « renseignements de base sur les clients » (p. ex., identificateurs de téléphone cellulaire, adresse IP). Ils ont laissé entendre que les types d'identificateurs de base demandés pour les services sans fil et Internet sont plus chers à produire que ceux des services de télécommunication ordinaires, en raison de la technologie perfectionnée utilisée. Les fournisseurs de services sans fil et d'Internet sont d'avis qu'ils ne devraient pas être forcés de fournir plus d'information que les autres FST utilisant des technologies de télécommunication ordinaires.

- Ils ont fait remarquer que les « données de base » habituelles, comme le nom, l'adresse et le numéro de téléphone des clients sont peut-être moins névralgiques du point de vue de la protection de la vie privée, que le sont d'autres types d'identificateurs. Ils ont souligné l'importance de faire en sorte que les clients comprennent qu'il existe un cadre juridique dans lequel cette information est fournie aux services de police.

- Ils ont également recommandé l'adoption de mesures de protection importantes en ce qui concerne les agents désignés, notamment la mise en place d'un processus pour limiter le nombre de points de contact, pour assurer l'uniformité et pour confirmer que les agents d'application de la loi qui demandent les NAC ont le droit de recevoir cette information. Certains ont également proposé de travailler avec les organismes d'application de la loi à l'élaboration d'un formulaire de demande normalisé pour les NAC afin de faciliter le processus.

- Ils ont dit qu'il est possible que les nouvelles dispositions doivent traiter différemment les petits et les grands FST. Les nouvelles mesures pourraient avoir une incidence importante sur les petits FST, notamment sur les ressources (par exemple, les FST devront peut-être recruter et former du personnel s'il y a une augmentation de la demande de communication des NAC, ou encore mettre à niveau ou informatiser leurs systèmes d'information).

- L'industrie redoute que le volume de demandes relatives aux NAC augmente considérablement par suite de l'adoption de nouvelles mesures législatives, en l'absence d'autorisation judiciaire préalable et elle craint aussi une augmentation correspondante des coûts pour les FST.

- Les participants ont signalé que l'industrie des télécommunications au Canada collabore depuis longtemps avec les organismes d'application de la loi. Ils ont reconnu que l'accès aux NAC est un outil important de protection de la société, pour ces organismes et ils ont souligné leur volonté de maintenir des relations positives avec le milieu de l'application de la loi.

- Ils ont souligné que les grands FST disposent de services de sécurité qui ont pour seul rôle de répondre aux demandes des organismes d'application de la loi et de se conformer aux ordonnances judiciaires; que les FST fournissent ces services par souci de sécurité publique, et que cette aide est très coûteuse.

<u>DÉFENSEURS DU DROIT À LA VIE PRIVÉE</u>

De façon générale, les défenseurs du droit à la vie privée ont reconnu que le manque d'uniformité en ce qui concerne la communication des NAC par les FST nuit à l'application de la loi. Par contre, ce problème ne justifie pas selon eux que l'on permette aux FST d'avoir accès à cette information sans qu'il soit nécessaire de présenter un mandat, situation que la plupart des représentants considèrent comme une violation des libertés civiles et du droit à la vie privée. Il importe de démontrer que l'accès à l'information est nécessaire; des représentants disent que, jusqu'à maintenant, cela n'a pas été prouvé. Plus que tout, ces représentants ont insisté sur l'importance d'inclure un mécanisme de contrôle approprié, dans le processus de divulgation des NAC , de préférence, une autorisation judiciaire préalable, afin de protéger le droit à la vie privée et les autres droits garantis par la *Charte canadienne des droits et libertés*.

- Selon ce groupe, le milieu d'application de la loi doit d'abord prouver clairement qu'il a besoin des NAC avant que le gouvernement envisage d'obliger les FST à fournir cette information sur demande. Ce groupe estime que, dans la plupart des cas, les services de police

peuvent obtenir l'information voulue par des méthodes d'enquête traditionnelles, y compris en recourant à des mandats ou à des ordonnances de production.

- La majorité des participants sont d'avis qu'une autorisation judiciaire préalable devrait toujours être exigée lorsqu'il s'agit de communiquer des renseignements personnels aux organismes d'application de la loi. Plusieurs ont laissé entendre que cette exigence dépend de la nature de l'information recherchée (p. ex., il ne serait pas nécessaire d'obtenir un mandat pour obtenir de l'information du domaine public ou des données de base, comme le nom, l'adresse et le numéro de téléphone). Certains défenseurs croient qu'il est raisonnable de mettre en place des options permettant l'accès aux NAC sans qu'il soit nécessaire d'obtenir une autorisation judiciaire préalable; toutefois, la plupart des participants estiment aussi que les organismes d'application de la loi doivent en faire plus pour prouver publiquement pourquoi il est nécessaire d'obtenir les NAC sans autorisation judiciaire préalable.

- Certains ont affirmé que des dispositions existantes du *Code criminel* et de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) fournissent à la police le cadre législatif et les pouvoirs requis pour enquêter sur des crimes, y compris les crimes sur Internet. Ils ont avancé qu'il fallait mieux sensibiliser les intervenants et s'efforcer d'améliorer la collaboration entre les FST et les organismes d'application de la loi.

- Certains ont proposé que le gouvernement envisage d'établir dans le *Code criminel* des mécanismes permettant l'accès à certains renseignements selon des critères moins rigoureux (p. ex., la création d'un mandat selon un seuil moins élevé) ou encore établissant un processus accéléré pour obtenir une autorisation judiciaire. D'autres étaient d'avis qu'il est contre-indiqué de réduire les critères compte tenu des renseignements personnels visés. Certains répondants s'opposent à l'idée de mettre en place un processus accéléré pour autoriser l'accès aux NAC, estimant que l'article 487.11 du *Code criminel* permet déjà de mener des fouilles sans mandat en cas d'urgence, notamment en cas de menace imminente contre une personne ou un bien.

- Certains estiment qu'en l'absence d'une autorisation judiciaire, il est important de bien définir les circonstances dans lesquelles les organismes d'application de la loi peuvent demander les NAC (p. ex., une liste précise des circonstances où les organismes d'application de la loi peuvent obtenir les NAC sur demande). Il faudrait justifier les circonstances où il est approprié de permettre l'accès aux NAC sur demande, sans mandat.

- Tout comme l'industrie, les défenseurs du droit à la vie privée craignent que les renseignements énumérés dans le document de consultation ne se limitent pas à ce que les membres du public considèrent habituellement comme des « renseignements de base sur les clients » (p. ex., identificateurs de téléphone cellulaire, adresses IP).

- Ils affirment que les identificateurs personnels, d'apparence inoffensive, peuvent exposer des renseignements de nature délicate s'ils sont combinés à d'autres informations. Par exemple, chaque élément d'information au sujet d'une personne peut être combiné d'autres renseignements afin de révéler des détails plus intimes sur celle-ci.

- Ils ont insisté sur la nécessité de mettre en place dans la loi de solides mesures de protection afin d'assurer un accès, une utilisation et une manipulation judicieux des NAC par les OAL. Ils ont dit craindre les « expéditions de pêche », ou la possibilité que les OAP accumulent et conservent des quantités énormes de renseignements personnels sur des individus. Ils ont donné en exemple les abus et irrégularités signalés récemment aux États-Unis en ce qui concerne les procédures administratives autorisant les fouilles. Certains participants estiment que les mesures de protection proposées dans le document de consultation étaient insuffisantes, peu importe le contexte, et que d'autres mesures de protection doivent être mises en place, même lorsque des autorisations judiciaires sont obtenues.

- Les participants ont indiqué qu'il est essentiel que tout modèle administratif établi par la loi (c.-à-d. accès sur demande, avec mesures de protection administratives) fasse l'objet d'un examen continu. Il faudrait aussi veiller à ce que tout changement sur le plan technologique ou dans la pratique ne mène pas à un processus qui contrevient à la *Charte canadienne des droits et les libertés* en empiétant indûment sur les attentes raisonnables en matière de droit à la vie privée.

- Un participant en particulier a proposé que la loi prévoie la création d'un groupe de travail, composé de représentants du gouvernement, de l'industrie, des groupes de défense du droit à la vie privée et de la société civile, qui aurait la responsabilité de formuler des conseils sur l'administration de toute mesure législative et de passer en revue les pratiques courantes.

<u>OBSERVATIONS DU PUBLIC</u>

La plupart des membres du public ayant présenté des observations s'opposaient à l'accès par les organismes d'application de la loi aux NAC en l'absence d'autorisation judiciaire préalable. Certains croient à tort que les organismes doivent actuellement obtenir une autorisation judiciaire préalable dans tous les cas. De façon générale, le public a l'impression que les organismes d'application de la loi cherchent à étendre leur champ d'activités d'une manière qui empiète sur la vie privée des Canadiens et Canadiennes

- Les répondants s'opposent fortement à ce que les organismes d'application de la loi aient un accès à l'information en ligne. Bon nombre croient à tort que les organismes d'application de la loi et de sécurité nationale cherchent à obtenir sans mandat un accès au contenu des communications, comme les courriels, ou à des renseignements sur les sites visités.

- Des membres du public ont avancé que, s'il n'est pas nécessaire d'obtenir une autorisation judiciaire préalable, il risque de se produire des abus, c'est-à-dire que l'on accèdera inutilement à des renseignements personnels. Ils ont fait des comparaisons en évoquant des abus et irrégularités signalés récemment aux États-Unis.

- Les membres du public étaient d'avis que rien ne démontre clairement que les organismes d'application de la loi ont besoin d'accéder aux NAC sans autorisation judiciaire préalable.

TAB B

Participants in the 2007 Customer Name and Address (CNA) Consultation include:

- Bell Canada
- British Columbia Civil Liberties Association
- British Columbia Freedom of Information and Privacy Association
- British Columbia Library Association
- Canadian Association of Chiefs of Police
- Canadian Association of Internet Providers
- Canadian Association of Research Libraries
- Canadian Bar Association
- Canadian Chamber of Commerce
- Canadian Resource Centre for Victims of Crime
- Canadian Wireless Telecommunications Association
- Canadian Internet Policy and Public Interest Clinic
- Dr. Avner Levin, Ryerson University
- Dr. Michael Geist, University of Ottawa
- Federal Ombudsman for Victims of Crime
- Information Technology Association of Canada
- International Perspectives
- Office of the Information and Privacy Commissioner of British Columbia
- Office of the Privacy Commissioner of Canada
- Office of the Information and Privacy Commissioner of Ontario
- Ontario Provincial Police, Child Pornography Section
- PovNet
- Rogers Communications
- Telus Mobility
- Yahoo! Canada

In addition, thirty-four submissions were received from the general public.

Les participants à la consulation publique au sujet de l'accès aux renseignements relatifs au nom et à l'adresse des clients (2007) comprennent :

- Bell Canada
- Association des libertés civiles de la Colombie-Britannique
- Freedom of Information and Privacy Association de la Colombie-Britannique
- Association bibliothécaire de la Colombie-Britannique
- Association canadienne des chefs de police
- Association canadienne des fournisseurs internet
- Association des bibliothèques de recherche du Canada
- Association du barreau canadien
- La chambre de commerce du Canada
- Centre canadien de ressources pour les victimes de crimes
- Association canadienne des télécommunications sans fil
- Clinique d'intérêt publique et de politique d'internet du Canada
- Dr. Avner Levin, Université Ryerson
- Dr. Michael Geist, Université d'Ottawa
- Ombudsman fédéral des victimes d'actes criminels
- Association canadienne de la technologie de l'information
- Perspectives international
- Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique
- Commissariat à la protection de la vie privée du Canada
- Commissaire à l'information et à la protection de la vie privée de l'Ontario
- Police provinciale de l'Ontario, La Section de la pornographie juvénile
- ProvNet
- Rogers Communications
- Telus Mobility
- Yahoo! Canada

De plus, trente-quatre soumissions ont été reçu du publique générale.

Pages 361 to / à 363

are not relevant

sont non pertinentes

Royal Canadian Mounted Police
Commissioner

Gendarmerie royale du Canada
Commissaire

Guided by Integrity, Honesty, Professionalism, Compassion, Respect and Accountability

Les valeurs de la GRC reposent sur l'intégrité, l'honnêteté,
le professionnalisme, la compassion, le respect et la responsabilisation

Protected "B"

The Honourable Stockwell Day, P.C., M.P.
Minister of Public Safety
269 Laurier Avenue West
Ottawa, Ontario
K1A 0P8

T.D. No / No. T.D.	022858
Routed to / Envoyé à	PAA
C.C	OMO, MO
B.F / A.R.	Nov. 27/07
File No / No. Dossier	7194-1

Dear Mr. Day:

Not relevant

[redacted]

Not relevant

[redacted]

The RCMP's National Child Exploitation Coordination Centre (NCECC) submitted a document entitled *Customer Name and Address Information Consultation (October 2007)* to the Public Safety and Industry Canada Consultation Panel. An Executive Summary is enclosed. It offers the most detailed explanation, to date, of the problems that the RCMP and Canadian police in general face in obtaining basic, non-sensitive customer information from Internet Service Providers (ISPs) and telephone companies. It also outlines the negative impact this has on law enforcement efforts to maintain public safety, and supports an administrative/regulatory model which provides a reasonable and balanced solution that merits full public consideration.

.../2

1200 Vanier Parkway
Ottawa, Ontario
K1A 0R2

1200, promenade Vanier
Ottawa (Ontario)
K1A 0R2

The NCECC submission demonstrates that the information in question is not sufficiently sensitive to require a warrant, and that the controversy over "CNA" (customer name and address) information has been miscast by the media. The pertinent public policy issue is how lawmakers can enable police to obtain that information while safeguarding individual privacy interests.

In cases where they have an IP address that was used or have found a cell phone at a crime scene, police are seeking to obtain the name or address of an unidentified customer from ISPs and/or telephone companies. An ISP or telephone company response indicates only who is responsible for, or is registered to the account, much the same as a license plate on a motor vehicle identifies the owner.

Obtaining a warrant for CNA information is not necessary under the law. In fact, the Supreme Court of Canada affirmed (in the *Plant* and *Tessling* cases) that a person's non-core biographical information does not attract a reasonable expectation of privacy. Therefore, it does not require the prior oversight and authorization of a court official for it to be released to police. Police recognize that CNA-type information is clearly personal information: personal information being any information that identifies a particular person. However, CNA personal information is not information that reveals intimate details about an individual and therefore its release to police does not need to be supervised by a court through a warrant process.

Furthermore, obtaining a warrant is not possible or practical in many cases. Obtaining warrants in the early stages of an investigation is not possible as police simply do not have sufficient grounds to apply for a warrant. In the performance of general policing duties, such as finding and notifying next of kin or locating overdue and missing family members, there is no criminal offence. Therefore, there are no grounds to apply for a warrant. Therefore, obtaining *timely* CNA information with a warrant in fast-moving, time-sensitive, or high CNA volume investigations, such as multi-million dollar Internet frauds, sexual assaults or other serious crimes in progress is not practical.

A warranted CNA regime would lead to tremendous strains on the judiciary and on law enforcement as telecommunication service providers process hundreds of thousands of CNA requests yearly.

.../3

Today, there are approximately 400 telecommunication service providers in Canada. Certain telephone companies, as well as ISPs, resist and regularly refuse to assist in this way. In this regard, the NCECC reports a 30% non-compliance rate with CNA requests. Statistics for non-child exploitation investigations are not available.

The following three real life examples highlight this concern:

47 unidentified persons violating children online in Canada

In a recent international child pornography investigation, Germany identified 28 countries where online child sexual exploitation was occurring. Two hundred (200) IP addresses associated with online child sex offenders using Canadian ISPs were sent to the RCMP in Canada to identify the location of these accounts. Once that basic information was obtained, investigators could then work to confirm the identity of the suspects and then obtain search warrants. Forty-seven of 200 requests made to ISPs were flatly refused. Those 47 leads reached a dead-end and could not be investigated, leaving the unfound victims vulnerable to further abuse and placing other children at risk.

Live, online child rapist identified with ISPs' help

An online investigator had been working undercover for several months in a virtual room where pedophiles met to trade child pornography. The investigator captured IP addresses and was able to identify the suspects by requesting the information from cooperative ISPs. One day, a man the investigator had previously identified, with the confidential and voluntary cooperation of his ISP, told the investigator that he was going to sexually assault his toddler daughter and wanted to know if the investigator wanted to watch. The investigator was able to summon help from the police of local jurisdiction who immediately went to the scene of the crime. If the investigator had been forced to seek a warrant to compel the ISP to provide the information, the little girl would have been raped again that night. Due to the cooperation of this ISP, police were able to rescue the girl without delay.

International Internet Fraud Investigation

.../4

[redacted]

As demonstrated in the preceding scenarios, investigations are now being seriously delayed or thwarted due to non-compliance with CNA requests. Public safety risks of both personal injury and economic harm, will increase without a timely and workable solution to the CNA issue. The proposed CNA administrative scheme provides strong checks and balances for the protection of privacy. It would also develop national consistency in the handling of this information, and a process that would enable internal and independent audits of information handling practices.

In closing, I want to express my appreciation to you for considering the significant impact that this proposed legislation will have not only on police investigations, but on public safety. Should you wish to discuss this matter further, I remain available to meet with you or, if you prefer, RCMP officials may be made available to meet with your Department to discuss the CNA issue.

Yours sincerely,

for William J.S. Elliott ADD

Enclosure

Questions and Answers

1. What is "CNA" information and why do police need it?

Answer: "CNA" stands for "customer name and address". In the telecommunications world, it is the name and street address of the person who subscribes to a telephone or Internet service. A request for CNA is often a starting point to follow an investigational lead. The address, phone number and name provided by the telephone or internet company informs police where they have to start looking to find and talk to victims, witnesses and suspects.

2. Why don't police just get a warrant when they want CNA information?

Answer: CNA is "personal information" that is not sensitive. It doesn't reveal intimate details about a person's life. The law doesn't require a warrant for this type of "tombstone" information. It is not information that the Supreme Court of Canada says police need a warrant for in order to obtain it legally. It would not be an effective use of police or court resources to require police to obtain warrants for information that is not sensitive enough to require a warrant. In addition, police can only obtain a warrant for the investigation of an actual offence. If they are carrying out general duties and no foul play is suspected--for example, trying to locate overdue hikers or a missing spouse--then applying for a warrant is not even possible.

3. Why don't ISPs and telephone companies cooperate and volunteer CNA information if a warrant is not required?

Answer: ISPs and telephone companies are subject to privacy legislation. There is a specific federal law that regulates how they must handle and protect their customers' "personal information". That law allows them to provide non-sensitive customer information to police. However, it does not require them to do so – this would require a statute or a court order. Without a legal obligation, or a court order to compel the provision of this information, companies are concerned about potential liability if information is provided voluntarily.

4. How many requests do police make for CNA and how many are refused?

Answer: Police do not track the number of these requests or refusals. There could be hundreds of thousands of such requests made in a year across Canada. Since April, 2007, the RCMP's National Child Exploitation Coordination Centre (NCECC) began to track the number of requests it makes to ISPs for CNA information and how many are refused. The number of requests per month has varied – in one month close to 400 requests were made and the next month the total was closer to 100. One-third of all CNA requests in child exploitation investigations are refused.

5. Would the proposed legislation give police new powers so they could avoid getting a warrant?

Answer: No. The new law would clarify for ISPs, telephone companies, customers and police what basic, non-sensitive information will be provided if police need it to perform their investigative or general duties. This law would not give police the power to intercept communications or spy on internet use without a warrant.

6. Aside from Canadian police services, who supports the proposed legislation?

Answer: Public Safety and Industry Canada officials recently held public consultations on legislative proposals for an administrative model that would require Internet Service Providers (ISPs) and telephone companies to provide only basic, non-sensitive subscriber information to police when it is needed to help them try to identify people. Key stakeholders who participated in this most recent consultation process, including representatives of ISPs and telephone companies, as well as the Privacy Commissioner of Canada and the Federal Ombudsman for Victims of Crime, found the proposals to be reasonable and indicated support for them. Keeping the proposals as part of the Lawful Access bill would broaden public dialogue on this subject. The RCMP anticipates that most Canadians would welcome the opportunity for a more public and well-informed dialogue about the CNA challenges facing police. Their support of these proposals, which are reasonable and ultimately serve public interest, is essential.

EXECUTIVE SUMMARY

NCECC – RCMP SUBMISSION TO PUBLIC SAFETY CANADA CUSTOMER NAME AND ADDRESS (CNA) INFORMATION CONSULTATION

The National Child Exploitation Coordination Centre (NCECC) of the RCMP participated in Public Safety and Industry Canada's recent public consultations concerning customer name and address (CNA). The main points of the NCECC submission, made on behalf of the RCMP, are summarized here.

Suitable legislation is essential to specify what customer identifying information Telecommunications Service Providers (TSPs) must provide to police upon request, as well as to ensure suitable privacy safeguards are in place for that information. Police have longstanding authority under the common law to ask people, including companies, questions in the lawful execution of their duties. But the common law does not require answers. Only legislation can compel TSPs to provide basic customer identifying information to police upon request.

While it is not standard practice in police operations to log instances where police requests to companies to voluntarily provide this information are turned down, NCECC recently began documenting such refusals to gauge the magnitude and impact of the problem. On average, one-third of all requests made each month to ISPs for basic CNA information are not being met. As a result, many child exploitation investigations never get off the ground, online offenders continue to offend and their child victims continue to suffer.

The debate surrounding police access to CNA in the media, so far, has concentrated on whether police should simply obtain a warrant. While, at first glance, this option might appear viable, it is not practical and would not serve law enforcement's operational needs or the public interest.

Police recognize that the information in question is "personal information"; however, it is not personal information that is sensitive. It does not reveal intimate details about someone's lifestyle and personal choices. The Supreme Court of Canada affirmed (in the *Plant* and *Tessling* cases) that a person's non-core biographical information does not attract a reasonable expectation of privacy and, therefore, does not require the prior oversight and authorization of a court official for it to be released to police.

Nonetheless, TSPs are often reluctant to volunteer CNA information. Some simply refuse to do so and tell police to obtain a warrant. To be able to continue their investigations, when police have sufficient information to obtain a warrant they will usually accede to the TSP's demand. On the other hand, applying for warrants, in situations where the law does not require them, appears to law enforcement agencies to be a poor use of limited police and court resources.

In cases, where the matter is in the early, "pre-warrant" stage of investigation, police simply do not have sufficient grounds to apply for a warrant. An ISP's refusal to

voluntarily provide a customer's name and address information at this stage of a child exploitation investigation often means the end of the investigation.

In addition, police do more than conduct investigations. They perform general duties -- such as finding and notifying next of kin or locating overdue and missing family members. Since general duties do not involve the investigation of an offence, at no time can a warrant be used to secure customer identifying information for these purposes.

Lastly, in addition to situations where obtaining a warrant for basic customer information is not at all possible, there are circumstances where obtaining a warrant is not feasible because the CNA information is needed immediately to prevent a serious harm from occurring. For example, an offender is inviting collaborators to watch him rape his step-daughter live on the Internet or an offender is accessing other people's non-secure wireless Internet connections to invisibly commit fraudulent financial transactions. In these circumstances, while police would be able to make out the grounds to obtain a warrant, by the time they would be able to do so, serious harm to a person or property would have occurred.

Considering the problems police encounter obtaining CNA voluntarily and the inadequacy of warrants as a solution, the RCMP and other police agencies have come to the conclusion that legislation is needed to oblige TSPs to provide basic customer identifying information upon request. This legislation must be administrative in nature – to accommodate all investigative and general policing reasons for seeking this information. Also it must incorporate various measures to safeguard privacy interests (such as detailing what information can be requested, who can request it, how it is to be recorded and handled), as well as to build in audit and accountability mechanisms.

Submission Prepared by:
Supt. Earla-Kim McColl
NCECC
In Collaboration with
Susan Alter, Counsel, RCMP Legal Services

27 October 2007

Public Safety Canada
Deputy Minister

Sécurité publique Canada
Sous-ministre

Ottawa, Canada
K1A 0P8

COPY

For your meeting with: Mr. Steve Sullivan, Federal Ombudsman For Victims of Crime

On: Tuesday, March 24, 2009 from 9:00 – 9:30 a.m.

SECRET

DATE: 2013/09

File No./TD No. 6950-13/360818

MEMORANDUM FOR THE MINISTER

MEETING WITH STEVE SULLIVAN,
FEDERAL OMBUDSMAN FOR VICTIMS OF CRIME

(For Information)

Issue

- You will be meeting with Mr. Steve Sullivan, Federal Ombudsman for Victims of Crime, on Tuesday, March 24, 2009, from 9:00 - 9:30 a.m.

Background

- The Office of the Federal Ombudsman for Victims of Crime was established in March 2007 to, among other things:
  - enhance awareness among policy makers of the needs and concerns of victims;
  - facilitate access for victims of crime to existing federal programs and services; and,
  - identify emerging and systemic issues that impact negatively on victims.

Canada

- The 2007-2008 *Annual Report of the Federal Ombudsman for Victims of Crime* (**TAB A,** refer to page 6) recommended, the introduction of legislation requiring Internet Service Providers to provide Customer Name and Address (CNA) information to law enforcement agencies as a mean to enhance their ability to combat the sexual exploitation of children on the Internet.

- During public consultations on Customer Name and Address (CNA) information in 2007, Mr. Steve Sullivan, as Federal Ombudsman for Victims of Crime, expressed the view that legislation in this area was needed. He again emphasized this need in a letter addressed to you dated February 16, 2009, attached at (**TAB B**).

- Mr. Sullivan's letter also expressed concern regarding a recent Globe & Mail article (attached at **TAB C**) which reported your comments to the effect that lawful access "legislation is not imminent."

Not relevant

- Under the *Personal Information Protection and Electronic Documents Act*, an organization may disclose personal information without the knowledge or consent of an individual if a government institution has 'lawful authority' to obtain requested information. As you are aware, there has been ongoing controversy surrounding the interpretation of 'lawful authority' in the *Personal Information Protection and Electronic Documents Act*. This has created difficulties for law enforcement officials accessing basic Customer Name and Address (CNA) information from service providers during criminal investigations.

Current Status

- On February 4, 2009 Private Member's Bill C-285 (*Modernization of Investigative Techniques Act*) was reintroduced in the House of Commons by Ms. Marlene Jennings M.P. This Bill would compel telecommunications service providers to build and maintain intercept-capable networks, and to disclose Customer Name and Address (CNA) information to law enforcement and the Canadian Security Intelligence Service upon request.

- [redacted]

- Public Safety Canada leads on the National Strategy for the Protection of Children against Sexual Exploitation on the Internet. The Department has established a strong partnership with the Canadian Centre for Child Protection, which manages Cybertip.ca, for the development of education and awareness materials related to child sexual exploitation. Cybertip.ca also acts as Canada's national tip line. The National Strategy is comprehensive in that it addresses legislative, policy, enforcement and prevention components of child sexual exploitation. Your recent announcement on Safe Internet Day respecting the renewal of the Strategy, reinforces the Government's ongoing commitment to combat this crime.

Considerations

- Mr. Sullivan may raise with you the issue of sharing, by the Royal Canadian Mounted Police (RCMP), of the personal information of victims of crime with provincial and territorial victim services agencies.

- Prior to 1999, provincial and territorial victim service personnel in some RCMP Detachments had access to the Police Information Retrieval System, and could review occurrence records to determine who to contact to offer victim services. The Office of the Privacy Commissioner of Canada advised that it did not consider the sharing of this information to be consistent with Section 8(2)(a) of the *Privacy Act*.

- Accordingly, the RCMP withdrew access to this information by victim services personnel and implemented a consent model whereby victims needed to consent to have their information released to victim services organizations. Victim services organizations, as well as provincial and territorial officials, have raised concerns they are experiencing reductions in the number of victim referrals as a result of this change in policy.

- [redacted]

Issues to Raise

- You may wish to highlight ongoing federal efforts to combat child sexual exploitation on the Internet, including the renewal of the National Strategy, to provide reassurance that the Government of Canada is strongly committed to addressing issues in this area.

- You may also want to emphasize the Government's commitment to provide law enforcement with the tools necessary to effectively investigate crime in the 21st century. Speaking points are attached for your consideration at (**TAB D**).

Recommendation

- It is recommended that Lynda Clairmont, Assistant Deputy Minister, Emergency Management and National Security, accompany you to the meeting.

Suzanne Hurtubise

Enclosures: (4)

Government of Canada / Gouvernement du Canada

The Office of the Federal Ombudsman for Victims of Crime | Le Bureau de l'ombudsman fédéral des victimes d'actes criminels

ANNUAL REPORT

ombudsman *n* (äm-budz-mun)
1. a public official appointed to investigate citizens' complaints against government agencies or officials that may be infringing on the rights of individuals 2. a person employed by an institution to investigate complaints against it that may be infringing

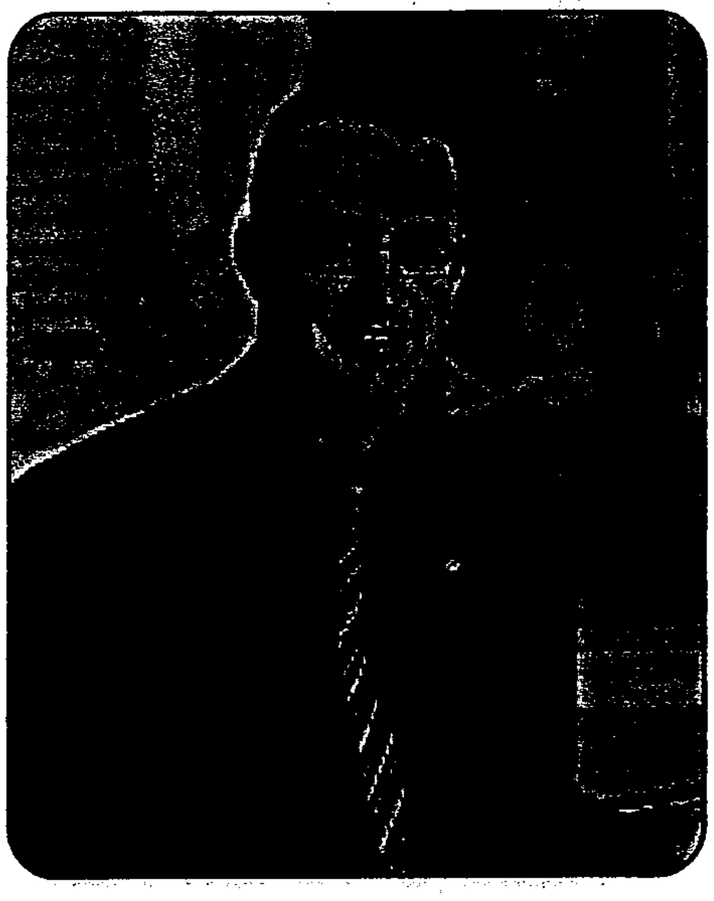
médiateur, personne chargée de la défense du citoyen contre les abus de l'administration

APRIL 2007 - MARCH 2008

Canada

TABLE OF CONTENTS

Message from the Federal Ombudsman for Victims of Crime



In April 2007, I was appointed Canada's first Federal Ombudsman for Victims of Crime by the Minister of Justice and the Minister of Public Safety. This Annual Report summarizes what has been accomplished in our first year and forecasts the work ahead.

It has been a challenging year – setting up a new, unique office while directing our energies to the essential mandate of responding to calls and enquiries from victims of crime across the country.

At the heart of this office's work is the historic *Canadian Statement of Basic Principles for Victims of Crime*. When federal, provincial and territorial ministers embraced the document twenty years ago, they dedicated their governments to consider the needs of victims of crime in developing new policies and legislation. Quite simply this means listening to victims, providing information while protecting their privacy and security and, above all, showing basic respect and compassion.

There has been a lot of progress for victims in Canada, but there is still much work to do. Over the last year, we have been successful in resolving a number of serious complaints from victims of crime. In other cases, we have helped victims find the assistance they need, by putting them in contact with someone in their community or a program in their province to help with the financial impact of crime.

The stories we hear from victims are too common.

Victims have called our office concerned that the person who victimized them was back in the community. Many of these callers were unaware they could register with the National Parole Board or the Correctional Service of Canada to find out when the offender was being considered for release or that they could take part in federal parole hearings. We have consulted with interested advocates and groups on how to better inform victims of their right to register. This issue will be part of a comprehensive report we are preparing for the Government regarding the *Corrections and Conditional Release Act*.

Victims of many different kinds of crimes tell us they suffer financial impacts as a result of these crimes, whether it is loss of wages, costs of counselling or loss of retirement funds. We have recommended that the federal government reform legislation to hold offenders financially accountable to their victims.

Victims have also told us they live in fear of when the offender is going to be released. One woman wrote to

say she is worried that she may not be informed if the man who attacked her is not deported. Over the next year, we will work with the Minister of Citizenship and Immigration to enhance the rights of victims in the deportation process.

Law enforcement officers have told us of their frustrations in trying to get information to track sexual predators on the Internet and identify and rescue child victims. We have recommended the Government address this information gap to help police better identify child victims. We will release a report in the near future recommending that the Government develop a national strategy to identify child victims in sexual abuse images, improve treatment for victims and regulate the role of Internet Service Providers to prevent revictimization.

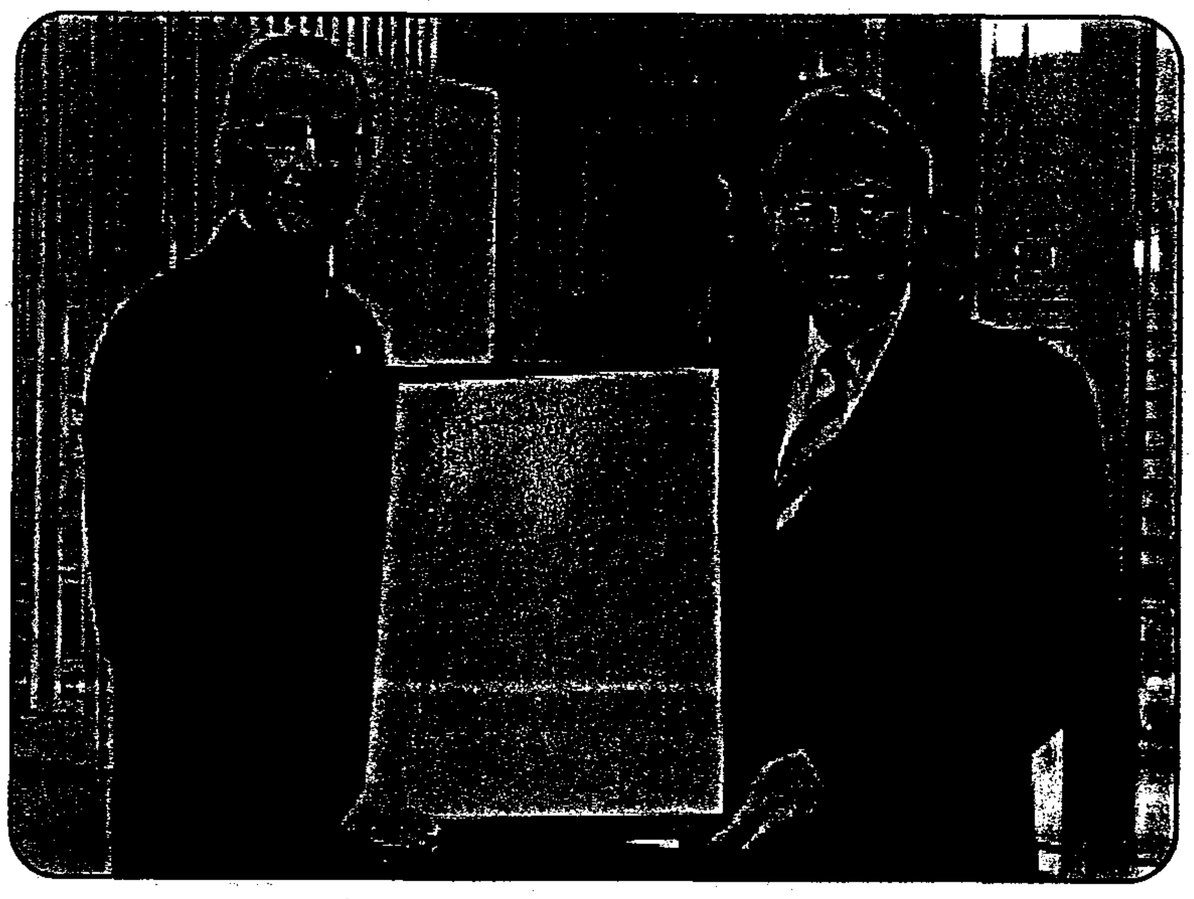
And there are many more areas we need to address. For instance, the rates of victimization in Aboriginal communities and the challenges these victims face are alarming. The treatment of victims within the justice system, despite the progress that has been made, is still not good enough.

Over the next year, our office will continue to respond to enquiries from victims. We will continue to make recommendations to the Government to identify systemic and emerging issues that impact negatively on victims. And we will work harder to make more victims aware of our office and the important services we provide.

Steve Sullivan
Federal Ombudsman for Victims of Crime

The family of a homicide victim was notified shortly before Christmas that the offender was granted a travel permit to visit his/her family over the holidays. The victim's family and offender's family live close to one another and the victim's family has seen the offender on other visits. Given the time of year, the victim's family was concerned about the impact the visit may have on their ability to celebrate Christmas. Although this office has no mandate to review the appropriateness of travel permits, we contacted the Correctional Service of Canada to let them know of the family's concern. The travel permit was changed and CSC officials agreed to meet with the victim's family to discuss their concerns.

Description of the Office of the Federal Ombudsman for Victims of Crime



Steve Sullivan, presenting the Honourable Rob Nicholson, Minister of Justice and Attorney General of Canada, with a framed copy of the *Canadian Statement of Basic Principles of Justice for Victims of Crime*

Overview

The Office of the Federal Ombudsman for Victims of Crime was created in March 2007 to play a central role in the Government of Canada's commitment to assist victims of crime. The Ombudsman and his staff possess a solid knowledge of the federal justice system which ensures that victims of crime have both a greater voice and access to available services.

Mandate

The Office of the Federal Ombudsman for Victims of Crime is an arms length organization within the Department of Justice. The mandate of the OFOVC relates exclusively to matters of federal jurisdiction.

The Ombudsman has the mandate of:

- promoting and facilitating access by victims to existing federal programs and services and providing them with information and referrals;
- addressing complaints of victims about compliance with the provisions of the *Corrections and Conditional Release Act* that apply to victims of offenders under federal supervision and providing an independent resource for those victims;
- enhancing awareness among criminal justice personnel and policy makers of the needs and concerns of victims and the applicable laws that benefit victims of crime, including to promote the principles set out in the *Canadian Statement of Basic Principles of Justice for Victims of Crime;*
- identifying emerging issues and exploring systemic issues that impact negatively on victims of crime.

Authority

Addressing the needs of victims of crime in Canada is a shared responsibility among all levels of government.

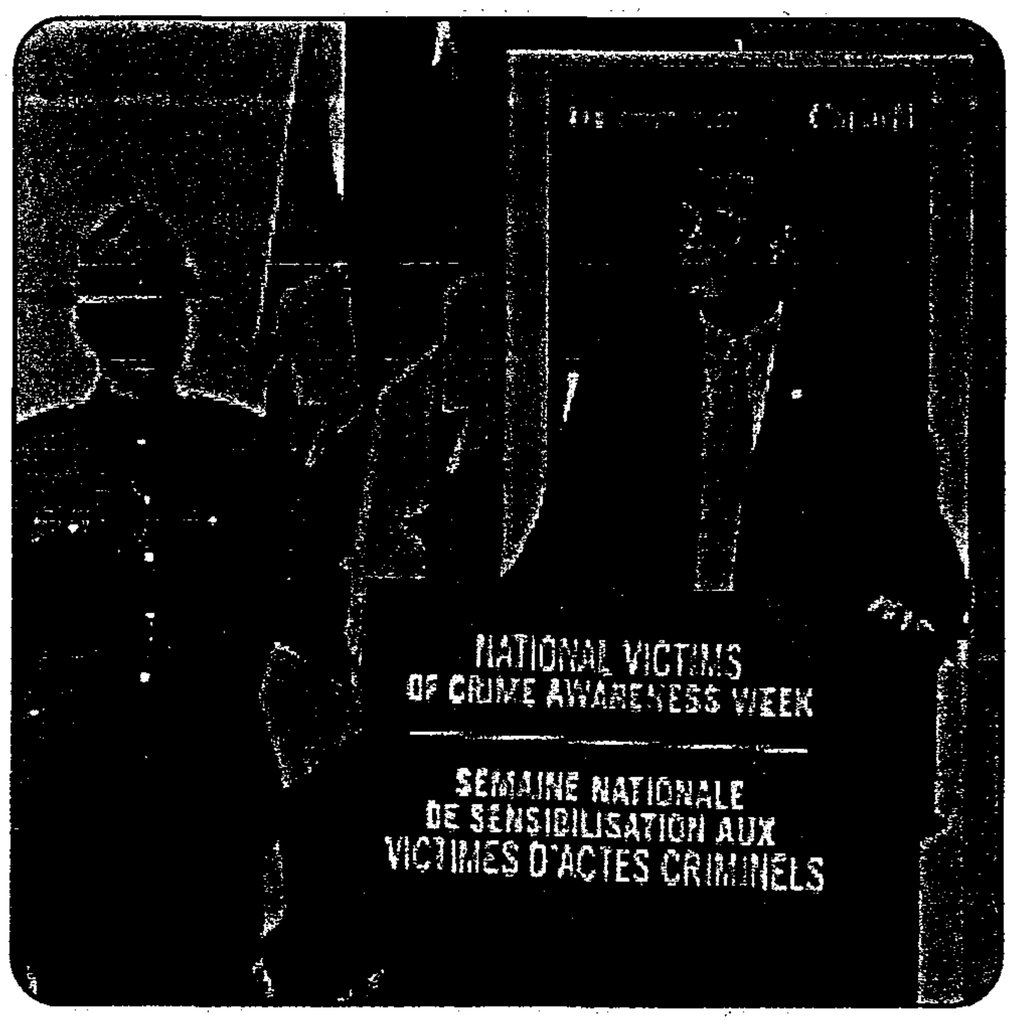
"An office like this is long overdue. Keep up the good work."

(Victim of Crime)

For the most part, delivery of victim services is undertaken by the provinces and territories as they have responsibility for the administration of justice. The Ombudsman will not encroach on the jurisdiction of the provinces or territories nor require them to implement or expand programs. The Ombudsman complements but does not replace the work of the federal Departments of Justice and Public Safety, including the National Parole Board and the Correctional Service of Canada.

A request for review may be brought to the Ombudsman by:

- A registered victim regarding their rights under the *Corrections and Conditional Release Act*; or
- Any victim, victims' service organization or victims advocate regarding other matters within federal responsibility.



Steve Sullivan, speaking at the official launch ceremony of National Victims of Crime Awareness Week

The Ombudsman must commence a review at the request of the Minister of Justice or the Minister of Public Safety. Additionally, the Ombudsman may commence a review on receipt of a request for a review or on the Ombudsman's own initiative.

Matters that occurred before the Office was established in March 2007 can be reviewed only upon request from the Minister of Justice or the Minister of Public Safety.

Individuals must have exhausted all other avenues for resolving their complaint (including, if applicable, mechanisms offered by the National Parole Board and the Correctional Service of Canada) before contacting the Office.

The Ombudsman may issue reports, including recommendations on specific matters, to the Minister of Justice or the Minister of Public Safety, depending on the issue.

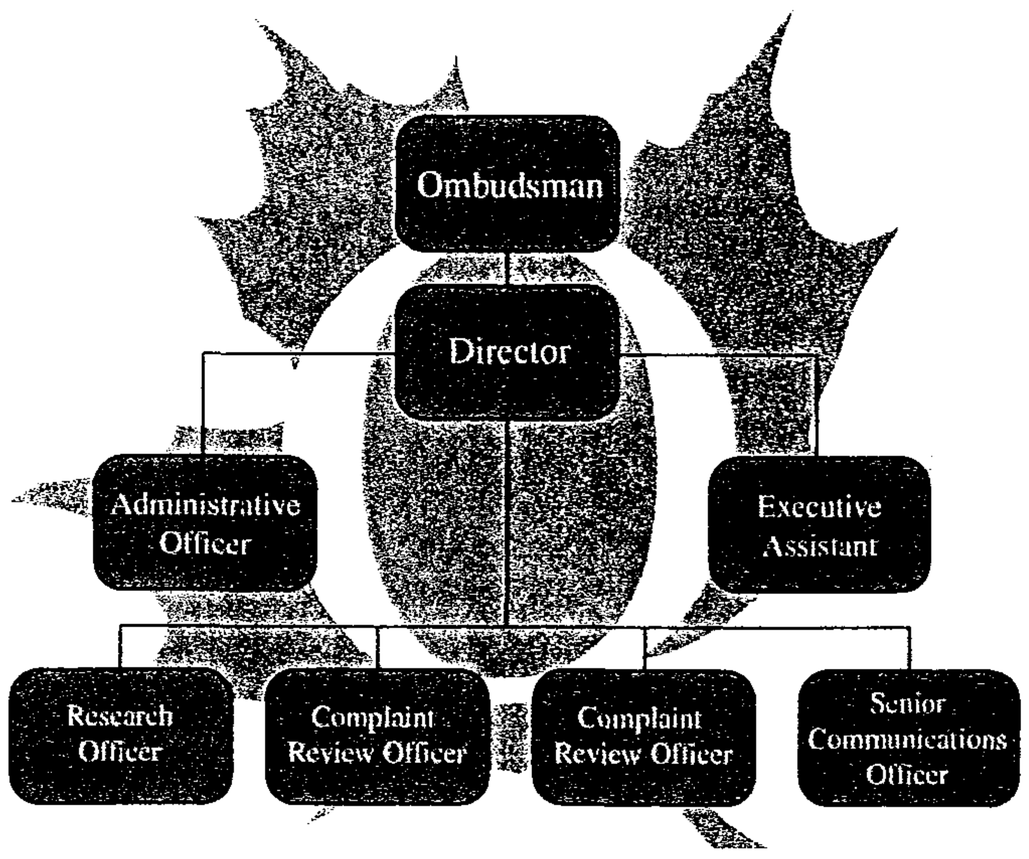
Although the Ombudsman's recommendations will not be binding, the Government will seriously consider the recommendations. The Ombudsman may request a response from the responsible department that indicates what action is contemplated or being taken with respect to the report's recommendations or explains why the recommended action will not be taken.

Human Resources

The Office was launched in 2007 and during the first year of its tenure, a core team of dedicated individuals was established to ensure that the Ombudsman would fulfill his mandate and respond to the concerns of victims. These professional and knowledgeable individuals came to the Office on secondments, interchanges, and casual work terms. While all positions have yet to be filled on a permanent basis, the staffing process is underway and is expected to be completed soon.

While maintaining its independence, the Office enjoys the Department of Justice's technical and administrative support services, and is grateful for their assistance.

Organization Chart



Highlights

Steve Sullivan, presenting the Honourable Stockwell Day, Minister of Public Safety, with a framed copy of the *Canadian Statement of Basic Principles of Justice for Victims of Crime.*

During the Office's inaugural year, the Ombudsman made several key recommendations to federal government departments on issues that impact negatively on victims of crime.

a) Correctional Service of Canada Review

On April 20, 2007, the Honourable Stockwell Day, Minister of Public Safety announced the appointment of an independent panel to review the operations of the Correctional Service of Canada (CSC) as part of the Government's commitment to protecting Canadian families and communities. The Ombudsman provided a written submission and met with the Review Panel.

The Ombudsman recommended:

- More information about offenders for victims of crime
- Serious consideration of Aboriginal victims' voices
- Greater care in sharing victim information with offenders to ensure utmost safety

The Review Panel released its report in October 2007 and said it had, "reviewed CSC's proposed implementation plan to ensure that it was responding to the Government's initiatives to support victims of crime and develop the human resource infrastructure required to deliver timely, accurate information to meet the needs of victims. An important part of the review was consultation with the recently appointed Federal Ombudsman for Victims of Crime, Steve Sullivan."

This Office is pleased to note that the Review Panel incorporated all of the Ombudsman's recommendations.

b) Internet-facilitated Child Exploitation

The Ombudsman participated in two government consultations to highlight the need for legislative reform that would enhance law enforcement abilities to identify victims seen in child sexual abuse images found online. Unlike other countries, Canada does not have legislation requiring Internet Service Providers (ISPs) to assist police to identify and rescue victims of Internet-facilitated sexual exploitation. Children are left vulnerable to future abuse if police cannot identify Internet users.

i) In the fall of 2007, the Department of Public Safety released a consultation document entitled *Customer Name and Address Information Consultation*, and the Ombudsman provided a written brief and met with the Panel. The Ombudsman recommended that the Minister of Public Safety introduce legislation requiring ISPs to provide customer name and address information to law enforcement agencies investigating Internet facilitated child sexual abuse cases.

ii) The Minister of Industry released a consultation document in response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics on the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The Ombudsman noted that PIPEDA permits organizations, such as ISPs , to disclose personal information without consent – but they are not required to. The Ombudsman recommended that the Minister of Industry proceed immediately to amend PIPEDA to require ISPs to provide the names and addresses of customers in investigations involving the abuse of children. The Minister made a commitment to amend PIPEDA to clarify that ISPs can legally share the information.

c) Restitution for Victims of Crime

In 2003, crime in Canada cost an estimated $70 billion – and the majority of those costs - $47 billion, or 67% – was borne by victims. A sentencing option called restitution – which promotes a sense of responsibility in offenders and their acknowledgement of the harm done to victims – is underutilized and poorly enforced in Canada. The Ombudsman has called on the federal government to review potential restitution options so that more offenders are held accountable to more victims. The Ombudsman has also made a concurrent recommendation that members of the judiciary become better informed about the challenges victims of crime face and the importance of both restitution and victim fine surcharges. The Ministers of Justice and Public Safety established a working group to examine the Ombudsman's recommendations.

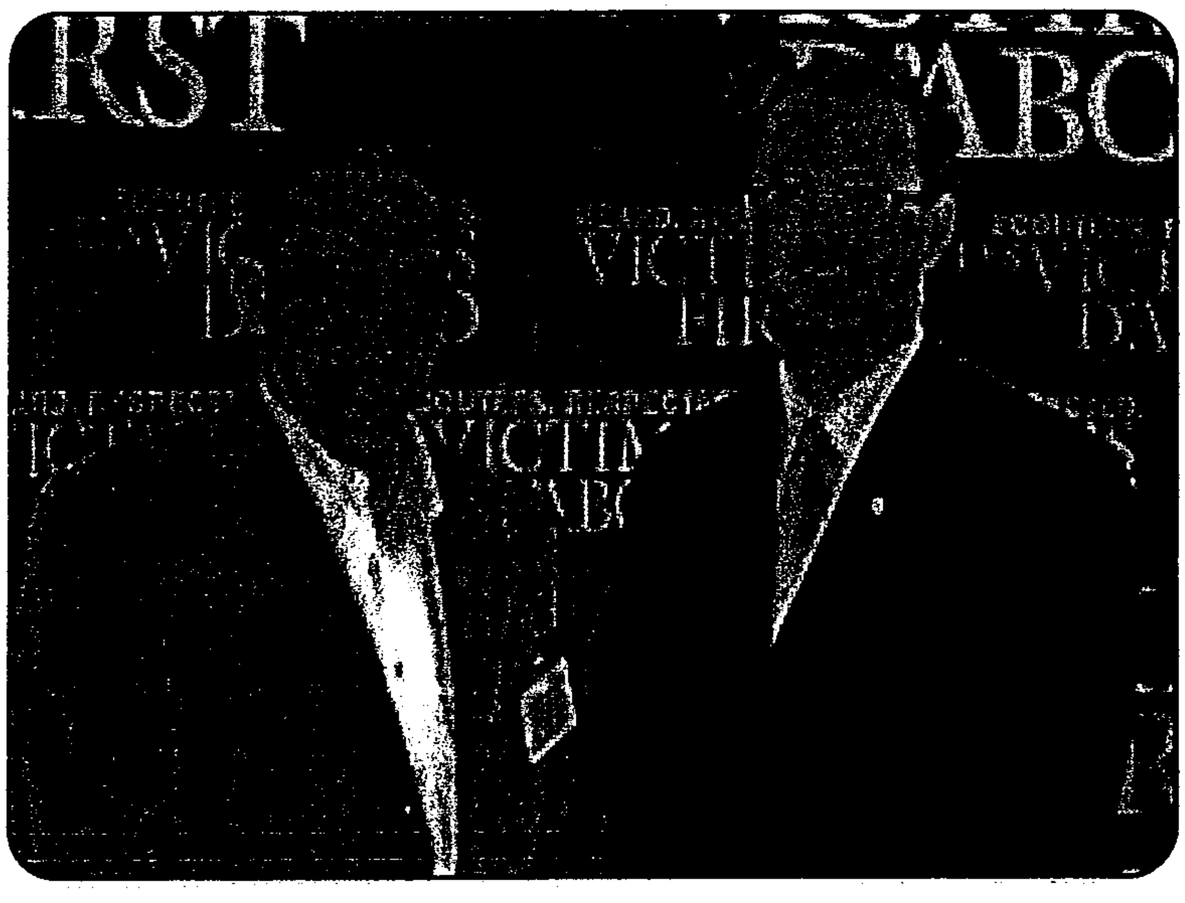
d) National Sex Offender Registry

The National Sex Offender Registry (NSOR) was created in 2004 to assist police investigations of child abductions and sexual offences. The Ombudsman's office expressed concerns to the Minister of Public Safety about its effectiveness and made several recommendations in order to strengthen its capacity as a useful tool for law enforcement to prevent crimes, protect children, and identify suspects.

Currently, in order to access the NSOR, law enforcement personnel must first determine if a specific crime is of a sexual nature. However, time is of the essence in many cases (for instance, in child abductions by strangers) and it is unreasonable to expect that this determination be made before the NSOR is accessed. The Ombudsman believes that access to the registry be enhanced so that frontline law enforcement personnel can access it on a timely and proactive basis, without having to wait for a formal determination whether the crime was sexually motivated. The Ombudsman recommended that the legislation governing the NSOR be reviewed by the relevant Parliamentary Committee in order to improve its capacity as a public safety tool. The Minister of Public Safety requested that the Standing Committee on Public Safety and National Security review the legislation.

The Ombudsman also noted that the Correctional Service of Canada did not always alert the Royal Canadian Mounted Police when registered sex offenders were released from prison. The Minister of Public Safety provided assurance that the Government was taking appropriate steps to improve the NSOR and that there is now an administrative agreement between the CSC and the RCMP to share information on the release of sex offenders.

Complaints



Sheldon Kennedy, former National Hockey League player and author of "Why I Didn't Say Anything", with Steve Sullivan at the official launch ceremony of National Victims of Crime Awareness Week.

The Office only addresses matters of federal responsibility and provides a thorough, impartial and independent review of complaints. The Ombudsman has the power to review, make recommendations to government and report publicly.

The Office of the Federal Ombudsman gives all parties in a dispute the opportunity to be heard and treats all individuals, government departments and agencies fairly, with dignity and respect.

Some examples of complaints the Office may review are:

- A registered victim was not provided with information as set out in the *Corrections and Conditional Release Act*;
- A victim was not treated with respect by a federal agency;
- A registered victim was not notified of the release of an offender;
- A registered victim was denied funding to attend a federal parole hearing;
- A Canadian victimized in another country was denied emergency funding.

Some examples of complaints the Office cannot review are:

- Decisions made under provincial jurisdiction such as provincial compensation, police investigations, and violations of provincial victims rights legislations;
- Decisions of the National Parole Board (i.e. releasing an offender);
- A decision made by a prosecutor regarding prosecution and/or a decision made by a judge pertaining to an offender's sentencing;
- A recommendation and/or decision made by the Correctional Service of Canada pertaining to an offender.

The Office has provided assistance and referrals to victims across the country.

Types of complaints received

During its inaugural year, the Office received more than 500 telephone calls and e-mail messages, many of which resulted in victims receiving information and referrals to appropriate agencies.

A large number of these contacts involved issues related to federal institutions such as the National Parole Board and the Correctional Services of Canada.

"I would like to thank your office for all the assistance you provided...when you are dealing with a system that generally just gives you the run around and passes the buck onto someone else until you feel like giving up, it is a refreshing change to deal with someone who gives you answers directly, speaks with sympathy and treats you like a human being."

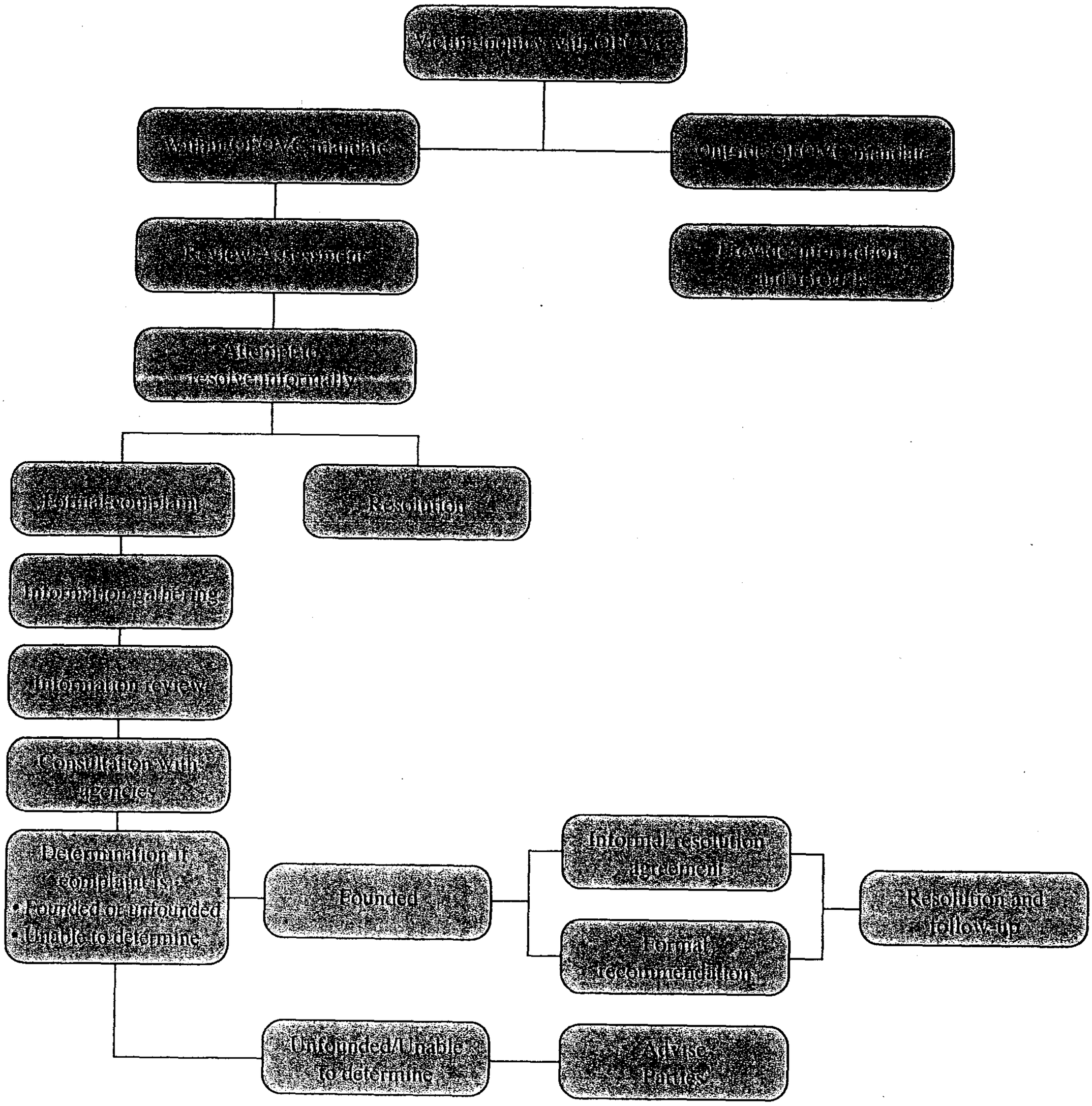
(Victim of Crime)

Logic Model 2007-2008

The following chart describes how the Ombudsman's Office operates and what outcomes are achievable.

How?	What do we want?		Why?
Key Activities/Outputs	**Immediate Outcomes**	**Intermediate Outcomes**	**Final Outcomes**
• Establish and promote the Office of the Federal Ombudsman for Victims of Crime and the services available to victims of crime and their families, and those who support them • Provide victims of crime and their families with support and information about victim services available to them and their role in the criminal justice system, and make referrals to appropriate offices and contacts • Review complaints from victims of crime and their families and make recommendations that will make federal government legislation, regulations, standards, policies, procedures and programs more responsive to the rights, needs and concerns of victims of crime and their families • Educate federal government departments about the rights, needs and concerns of victims of crime and how to be more responsive	• Victims of crime and their families, and those who support them, are more aware of Office of the Federal Ombudsman for Victims of Crime and its services • Victims of crime and their families are more aware of the services and assistance available to them and their role in the criminal justice system • Increased awareness and understanding of changes needed to federal government legislation, regulations, standards, policies, procedures and programs to make them more responsive to the rights, needs and concerns of victims of crime and their families • Increased awareness and understanding of how to better address the rights, needs and concerns of victims of crime and their families within the federal government	• Victims of crime and their families are able to make better informed decisions about accessing services available to them • Federal government legislation, regulations, standards, policies, procedures and programs are more responsive to the rights, needs and concerns of victims of crime and their families	• Victims of crime are better served and supported by the federal government • A fair, relevant and accessible justice system that reflects Canadian values

Inquiry and investigation process



Communications and Outreach

The Ombudsman feels it is important that Canadians, and especially victims of crime, be aware of the Office and the services it offers. During this first year of operation, important steps were taken in this direction.

Awareness

The Ombudsman travelled extensively across Canada to meet with victims and victim services providers to build relationships and to hear their stories. Productive meetings were held with community-based and police-based victim services providers, Aboriginal groups such as the Native Women's Association of Canada, and governmental partners such as the Department of Justice's Policy Centre for Victim Issues.

Communications

Information packages were provided to victims and services providers as well as federal partners such as the Correctional Service of Canada, the National Parole Board, the Royal Canadian Mounted Police, the Canada Border Services Agency, Indian Residential Schools Resolution Canada, and the Department of Foreign Affairs and International Trade.

Web Site and Logo

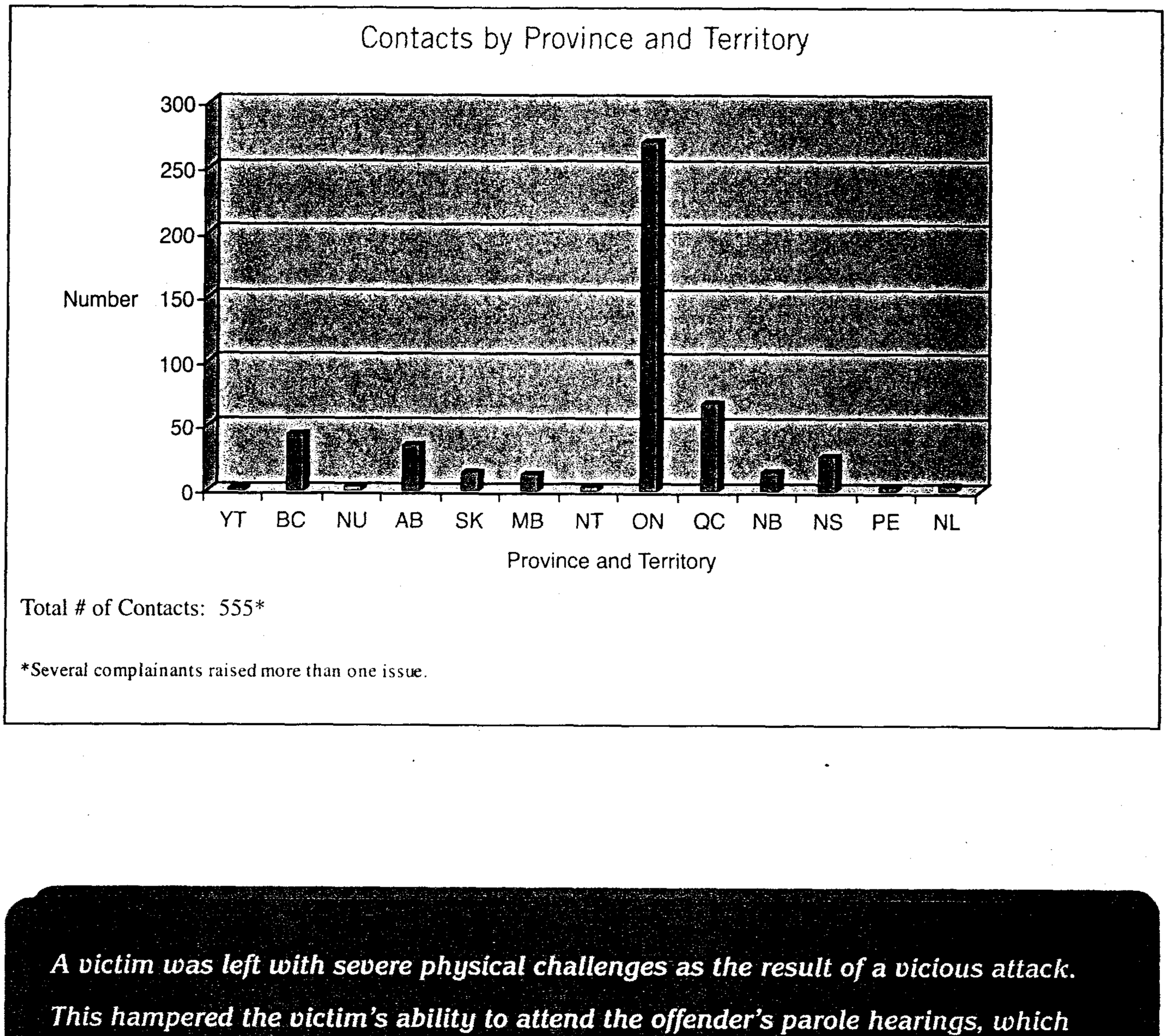
The Website and logo respect the Government's common look and feel, eye-catching and easy to navigate.

Events

The Ombudsman took part in activities surrounding the National Victims of Crime Awareness Week and other conferences and roundtables to promote the role of the Office and its services.

Networking

Presentations were made to share information on Canada's victim services strategies and to compare international best practices. Valuable links and connections were established with other service providers located outside of Canada.



Total # of Contacts: 555*

*Several complainants raised more than one issue.

A victim was left with severe physical challenges as the result of a vicious attack. This hampered the victim's ability to attend the offender's parole hearings, which were taking place in another part of the country, and to present a victim impact statement. The victim contacted our office to see if we could provide assistance. By working collaboratively with the National Parole Board, this office is very pleased to note that the victim was given the opportunity to attend the parole hearing through videoconferencing, a first for victims of crime in Canada. As a result of this case and our intervention, the NPB is working towards making videoconferencing an option for more victims.

About the Ombudsman

Steve Sullivan, a long-time advocate for victims of crime, was named by Order in Council to the position of the first Federal Ombudsman for Victims of Crime and took office in April 2007.

Mr. Sullivan began working in the victims' rights movement in 1993 as Director of Research with Victims of Violence, a national non-profit organization dedicated to the prevention of crimes against children. He held the positions of Executive Director, President, and Chief Executive Officer during his tenure with the Canadian Resource Centre for Victims of Crime, which is devoted to advocacy for victims and survivors of violent crime in Canada.

Mr. Sullivan has advocated on behalf of individual victims at different stages of the criminal justice system including the corrections system, and has worked with various levels of government for increased victims' rights and services. He has appeared before several government committees examining issues such as parole reform, legislation regarding the protection of children, sentencing reform, DNA evidence and victims' rights.

Mr. Sullivan holds a B.A. Honours in Law with a concentration in Criminal Justice from Carleton University.

A victim made an official complaint to the Office after realizing that his/her personal information (address and contact information) was accidentally shared with an offender through a Victim Impact Statement that he/she had provided for sentencing purposes. This victim was concerned enough for his/her safety that he/she was considering moving from their residence. The Office assisted the victim by liaising with the Correctional Service of Canada. The victim was satisfied with the resolution and the Correctional Service of Canada reviewed all of their files in order to minimize the risk of this happening to another victim.

Financial Statement

Summary of Expenditures (April 1, 2007 to March 31, 2008)

	ACTUAL
Salaries and employee benefit plan contribution	$320,283.00
Travel Expenses	$ 49,884.00
Training and professional dues	$ 12,285.00
Communication and public Outreach	$ 5,534.00
Office Set up	$ 29,736.00
Office furniture	$ 4,401.00
Professional and special services	$111,208.00
Rentals	$ 9,229.00
Materials and Supplies	$ 9,473.00
Acquisition of Computers and other equipment	$ 6,659.00
Miscellaneous	$ 271.00
Total	$558,910.00

The Office of the Federal Ombudsman for Victims of Crime | Le Bureau de l'ombudsman fédéral des victimes d'actes criminels

Heard. Respected. Victims First. | **Écoutées. Respectées. Les victimes d'abord.**

1 866-481-8429
www.victimsfirst.gc.ca
www.victimesdabord.gc.ca

Arsenault, Roger

From: Malone, Chantal
Sent: Tuesday, March 03, 2009 2:03 PM
To: Arsenault, Roger
Subject: vanloan-cna-feb09

Please log into CCM and have a recommendation drafted

Thanks

Federal Ombudsman for Victims of Crime

P.O. Box 55037
Ottawa, Ontario
K1P 1A1

Ombudsman fédéral des victimes d'actes criminels

C.P. 55037
Ottawa (Ontario)
K1P 1A1

February 16, 2009

The Honourable Peter Van Loan, P.C., M.P.
Minister of Public Safety
269 Laurier Avenue West
Ottawa, ON
K1A 0P8

Dear Minister Van Loan:
It was a pleasure to meet you on January 22, 2009, to discuss the work of our office and some of our priorities. As you will recall, we highlighted some of the recommendations of an upcoming report our office will be presenting to you and the Minister of Justice. The Report, entitled *Every image, Every Child*, will give an overview of the problem of Internet-facilitated child sexual abuse and will identify issues and the negative impact this horrific crime has on child victims. One of the issues highlighted in the Report will be the challenges law enforcement sometimes faces ~~to acquire~~when trying to acquire subscriber information from Internet Service Providers.
There are literally millions of photos and videos of child sexual abuse on the Internet today. These are not harmless photos of naked children; they are horrific images of innocent children being violently sexually abused. Sadly, the victims are getting younger and the abuses more violent.

At a roundtable held in 2007, my office asked law enforcement representatives to identify the biggest obstacles they face in identifying and charging those who create, distribute and trade child sexual abuse images and videos over the Internet. The obstacle identified hands down above all others was the inability to get basic subscriber information to link an IP address to a location or individual. Although most ISPs will cooperate with law enforcement requests in cases involving child sexual exploitation cases, 30 to 40 per cent of these requests are still declined and, as a result, investigations ~~are~~ may be terminated.~~are turned down.~~

A 2007 Department of Public Safety consultation document on customer, name and address information warned that, "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).*"

I was encouraged by your comments last week when you said that you were considering legislation to provide law enforcement with the tools they need to enforce the law in the age of the Internet. I agree with your comments that, "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."

However, I was equally concerned when, the following day, you were quoted in the Globe and Mail as saying legislation is not imminent. The need to rescue children from being sexually abused, Minister, is not only imminent, it is urgent.

I am concerned about some of the misinformation that may impact the public's perception of the Government's intention. For example, in response to a recent Ontario Superior Court decision that ruled subscriber information was not private, one privacy advocate suggested "It is not just your name. It is your whole Internet surfing history." This is absolutely false.

The Supreme Court of Canada has stated 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." As Justice Lynne Leitch of the Ontario Superior Court said in a very recent decision, "One's name and address or the name and address of your spouse are not biographical information one expects would be kept private from the state."

Under the current law (PIPEDA), ISPs are permitted, but not legally obligated, to cooperate and give this basic information to authorities. But if ISPs are permitted to provide a customer's name and address, it cannot be a violation of privacy if they are all forced to do so.

To rescue children and find offenders, police need this information and, as you rightly pointed out, in some cases, time is of the essence. In February 2009, law enforcement in Ontario arrested over 30 men during a province wide sweep. As part of the case, police removed a 12 year old girl ~~was removed~~ from the home of one of the men arrested on suspicion of distributing child sexual abuse images. If it were not for the arrest ~~but at the time of his arrest~~, law enforcement would have had no reason to believe the man was abusing this child.

I understand that the legislation you spoke of when you appeared before the Standing Committee on Public Safety and National Security deals with the broader issue of giving law enforcement the ability to "eavesdrop" on Internet exchanges. I am concerned that the two issues (warrants for access and CNA information) run the risk of confusing the public (the former needing a warrant and the latter not). Therefore, in order to ensure that measures to protect children from those who abuse them and distribute their images are put in place, I recommend you separate the two issues and expedite legislation to require ISPs to release CNA information to law enforcement without a warrant. This is not a privacy issue; it is a child safety issue.

I would be more than happy to meet with you to discuss this further at your earliest convenience.

Thank you.

3/3/2009

Sincerely,

Steve Sullivan
Federal Ombudsman for Victims of Crime

3/3/2009

Privacy watchdog warns Tories against mass snooping

BILL CURRY
The Globe and Mail
February 13, 2009

OTTAWA — Privacy Commissioner Jennifer Stoddart delivered a stern warning to the federal government yesterday, saying she is strongly opposed to any legislation that allows the "mass surveillance" of private e-mails and phone calls.

She was reacting to the news that the government wants to update Canada's wiretapping laws with new police powers to monitor criminal suspects in the digital era of cellphones and chat rooms.

"My concerns are a huge increase in surveillance powers," said Ms. Stoddart, who has been raising objections since such an update was first proposed in legislation in 2005 by the Liberal government of Paul Martin. The commissioner, who has had general discussions with federal officials and has been monitoring developments in other countries, said she expects to be consulted on any federal legislation.

"The [obtaining] of a warrant for looking into people's private papers, private affairs, now e-mail conversations is a basic tenet of our democratic and constitutional rights in Canada. To erode this is a very serious step toward mass surveillance so I would like to get a copy of any draft legislation and look at how this could be possibly justified. I've said in the past I've seen no compelling argument put forward for its justification."

Public Safety Minister Peter Van Loan told a Commons committee Wednesday that his government would propose "changes to programming and legislation" that would modernize police powers to catch criminals using modern devices.

Yesterday, the minister stressed that he supports Ms. Stoddart's concerns and that legislation is not imminent.

"We can't allow new technologies to defeat law enforcement. We have to protect our communities," Mr. Van Loan said. "That being said, we also have to make sure that whatever solutions we come up with respect privacy rights of law abiding Canadians. ... The concerns of the Privacy Commissioner are quite legitimate. We don't want to have legislation that intrudes on privacy rights and I can assure you we wouldn't come forward with that kind of legislation. But we also need to find a way to address a very real problem that's out there."

Opposition critics said they share the commissioner's concerns and would want to see the details of any legislation before taking a position.

Should the government move ahead, it could present an interesting political dynamic in the minority House of Commons.

The Liberals faced considerable resistance in government from Ms. Stoddart and other privacy advocates when they attempted a "lawful access" law in 2005. But a new private member's bill suggests Liberals and Conservatives may not be far apart on this issue.

Last week, Liberal MP Marlene Jennings introduced a 33-page private member's bill that is similar to what the Liberal government proposed. The legislation even carries the same title: the Modernization of Investigative Techniques Act.

The Liberal bill would force Internet service providers to be technologically equipped to allow police to "intercept communications and to provide subscriber and other information without unreasonably impairing the privacy of individuals."

Speaking Points

- Child sexual abuse of any kind is a horrifying crime.

- The Government is committed to providing law enforcement with the tools they need to combat this crime while respecting the privacy interests of individuals and victims of crime. Officials are considering how best to address this challenge.

- The Government of Canada remains committed to the global fight against the sexual exploitation of children and we will continue to work with our domestic and international partners to address this terrible crime.

- As a reflection of our commitment, on February 10, 2009, the Government announced the renewal of the *National Strategy for the Protection of Children from Sexual Exploitation on the Internet,* which will further help us combat child victimization and increase our capacity to investigate and track down on-line predators.

If asked about RCMP information sharing with Victim Services Groups

- We are working with our partners who include provincial and territorial governments, victim service organizations, and the RCMP to ensure victims are provided information about available victim assistance services and programs in a timely manner.

- We are also cognizant of our need to respect the privacy of victims and comply with the Federal *Privacy Act*.

Pages 400 to / à 407

are not relevant

sont non pertinentes

Public Safety Canada / Sécurité publique Canada

ACTION REQUEST / FICHE DE SERVICE

File / Docket No. – N° dossier

To / À:	Minister	Date:	May 4, 2009

Purpose / Urgency – But / Urgence

Information

Subject / Remarks – Sujet / Remarques

Customer Name and Address Information (CNA)

C.C.:		
	☐ Chantal Bernier	☐ Elisabeth Nadeau
	☐ Daniel Lavoie	
	☐ Lynda Clairmont	
	☐ Richard Wex	☐ Caroline Fobes
	☐ Kristina Namiesniowski	

Consultations undertaken / Consultations entreprises :

Legal / Services juridiques _____

Corporate Management / Gestion ministérielle _____

PCO-IGA / BCP-AIG _____

	Name/Signature Nom/Signature	Date
Originator Initiateur	Yacine Touizrar	May 4, 2009
Director Directeur		
Director General Directeur général	Nicole Ladouceur	
SADM/Assoc. ADM, EMNS SMAP/SMA déléguée, GMUSN	Lynda Clairmont	MAY 1 1 2009
ADM, CSPB SMA, SPP		
ADM, CMB SMA, GM		
Comptroller Contrôleur		
ADM, PLEIB SMA, SPALI		
ADM, SPB SMA, DPS		
Ministerial Services Division Division des services ministériels		
Associate Deputy Minister Sous-ministre délégué		
Deputy Minister Sous-ministre	Suzanne Hurtubise	

Revised

PS-51-E (2/05)

Pages 409 to / à 412

are not relevant

sont non pertinentes

PROTECTED
DRAFT – For Discussion

Customer Name and Address Information (CNA)

What is CNA?

CNA information refers to non-biographical identifiers (e.g., name, address, telephone number, Internet Protocol (IP) address, e-mail address, and wireless telephony subscriber service identifiers) that can help Law Enforcement Agencies (LEAs) and the Canadian Security Intelligence Service investigate specific offences and discharge their broader public safety mandates. Currently, unless a request is made pursuant to section 184.4 of the *Criminal Code* (Exigent Circumstances), telecommunications service providers (TSPs) are not compelled to divulge this information to designated officials unless they have a warrant, and often refuse to do so due to client-provider privacy agreements.

Why a Warranted Regime is Ineffective

For LEAs, obtaining a warrant is often not an option. Warrants are only granted for criminal investigations where the identity of the suspect has been clearly established. There are many cases where police have reasonable grounds to believe that someone has committed a crime, but cannot obtain a warrant because they cannot identify the suspect (even though they may have a telephone number or IP address). There are also cases where "victims" need to be identified in non-criminal situations. Unfortunately, many TSPs will refuse to answer police requests for information pertaining to these individuals.

There are other cases where acquiring a warrant is simply impractical. The warrant process involves the investigator explaining his or her credentials, the history of the investigation, the criminal offence being committed and how it has been proven. This can take several hours, and once it has been completed, the warrant request goes through several officials before it can officially be executed. In many cases, completing this process would compromise or even jeopardize an investigation.

There is also a danger that a warranted regime could set a precedent that could further limit the effectiveness of the police by compromising police access to a great deal of information that the they use today on a daily basis, without which law enforcement would be seriously impaired. For example, if the police are required to get a warrant for subscriber information, why shouldn't they get a warrant before accessing CPIC, which contains much more private information than a customer's name, address and phone number?

Another significant concern would be that requiring a warrant may create problems for other government bodies that currently access this type of information in other contexts. For example, customs officers, immigration officers, fishery and wildlife services, and census officers, among others, currently request and receive a significant volume of personal information in order to perform their duties, and these officials are not required to obtain judicial authorization for doing so. These practices could subsequently be challenged as unsatisfactory were the government to require judicial pre-authorization for law enforcement access to phone-book type information.

A warranted regime would also place an unnecessary burden on the justice system. There are tens if not hundreds of thousands of subscriber information look-ups done annually, at all times of the day and night. Requiring a warrant would therefore be impractical from a resources and logistical point of view.

In addition, requiring a warrant would be problematic for police when they undertake non-criminal, general policing duties. For example, when the police seek to contact next-of-kin in a traffic accident, or an individual whose home has been broken into, or the family of an Alzheimer's patient who has wandered off, the individuals being contacted have not engaged in criminal acts, nor are they the subject of investigation. To create a legal threshold sufficiently broad to encompass the myriad situations in which a police officer may need to seek a name, address or phone number, and to include such a provision in the *Criminal Code*, was determined to be at a minimum inadvisable, perhaps even impossible.

In essence, should a warranted regime be pursued, given the above circumstances, and given that in other instances this type of information is often required at the early stages of an investigation (where the suspect's name is not even known), the threshold for issuance of such a warrant would have to be so low as to render the process essentially meaningless. This very basic information needs to be available when it is relevant to an investigation or general policing duties.

Given the necessity of such a low threshold for a warrant to access subscriber information, an administrative regime (non-warranted) with privacy safeguards would arguably provide greater transparency and accountability.

Scenarios in which a Warranted Regime is Ineffective

A. Cases Where Obtaining a Warrant is Impossible

Customer Name and Address

- **Identity of a Suspect**

Informants will often provide authorities with the first name or nickname and phone number of a suspect. This information is important in the early stages of an investigation. Checking a phone number against information provided by a TSP is invaluable because it can confirm or refute the informant's information and help lay the foundation for a successful investigation.

- **Child Luring over the Internet**

When police suspect that a child has been lured over the Internet to meet a suspicious adult, there is very little time to act. Police therefore rely on immediate access to the name and address of the person associated with the e-mail to pursue the investigation.

- **Missing Children**

When a child goes missing, the child's e-mail messages on the home computer may be a source of valuable information. One could discover that the child had arranged to meet a certain person (unknown name) at a certain spot. However, without additional information or reason to believe foul play, police would not have sufficient grounds to obtain a warrant to compel the TSP to disclose the full name and address of the person. Although some TSPs will agree to cooperate in these cases, unfortunately, other TSPs currently refuse to provide this information to the police, because of client-provider privacy agreements.

- **Crisis Line**

When threats of suicide are uttered over help lines, call display is not enough to determine the name and address of the persons calling. Police cannot obtain a warrant for this because an offence is not being committed. TSPs currently do not have to provide subscriber information to police in these cases, even though lives may be at stake.

- **Identity of an Incapacitated Person**

In situations where an unidentified person is incapacitated and is carrying only a cellular telephone, the police need to obtain the information associated with the person's cellular telephone, such as the person's name and address, to enable them to contact next of kin.

- **Accidents**

Law enforcement agencies sometimes require the assistance of TSPs to help identify the civic address of a rural resident, in cases, for example, where a driving accident victim's driver's license would only show a mailing address.

- **Property Recovery**

Law enforcement agencies require TSPs' cooperation to obtain the address of a person who has had their property stolen, in order for them to be able to return the goods upon completion of the investigation. A warrant is impossible to obtain in these circumstances because returning these items is not part of the criminal investigation.

Customer's IP Address

- **Child Luring over the Internet**

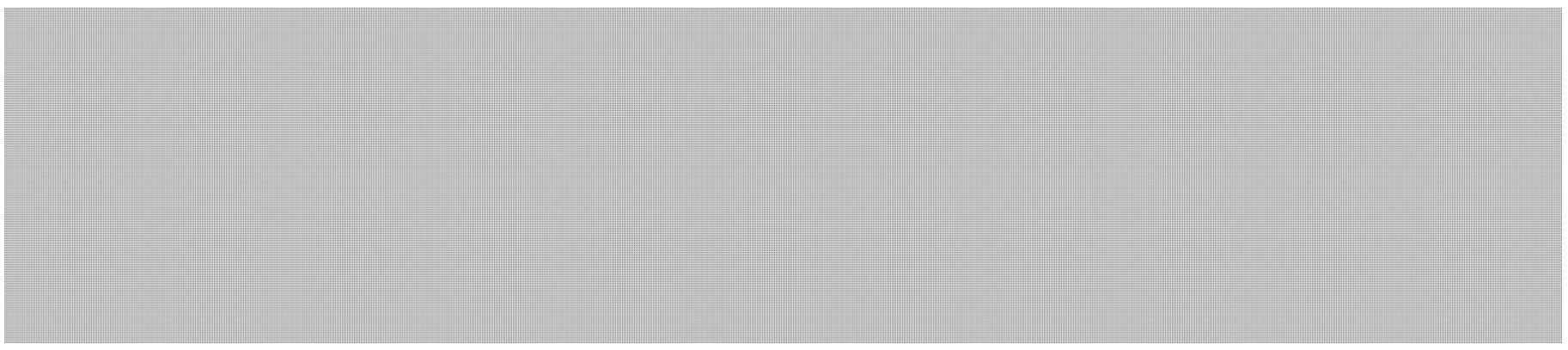
The RCMP's National Child Exploitation Coordination Centre (NCECC) often receives tips about Internet child luring, but can only identify the suspect by an on-line username. Without additional subscriber information, such as the suspect's IP address, the NCECC cannot determine the appropriate jurisdiction for the investigation. TSPs are not currently compelled to divulge the IP address in these situations and, and as a result, investigations are compromised.

- **On-line Pharmaceutical Sales**

Police are often called to investigate companies who are selling pharmaceutical drugs on-line. The operation of an on-line pharmacy providing prescription services to American and Canadian customers directly is a contravention of provincial as well as federal legislation (*Controlled Drugs and Substances Act*). The myriad of Internet routings, IP addresses and Internet Domain registrations, makes the tracing of finances a very difficult task. The ability of police to have immediate access to the subscriber information relating to the IP addresses is vital to these types of investigations.

B. Cases Where Obtaining a Warrant is Impractical

Customer Name and Address



- **Child Porn on the Internet – General Investigations**

Subscriber information is an essential stepping-stone in the beginning of a child pornography investigation. While police may have a list of IP addresses that have uploaded or downloaded child pornography from a server, they are unaware of the name and addresses of the subscribers to these addresses. For obvious reasons, it is impractical for police to apply for a warrant to obtain the names and addresses of the suspected child pornographers (based on the IP addresses), as valuable time is lost in this process.

- **Child Porn on the Internet – Establishing Jurisdiction**

In a recent project, the NCECC was given a list of 200 Canadian IP addresses that belonged to suspects who had purchased child pornography on-line from a foreign server. The NCECC had to trace the IP addresses provided by the foreign police services in order to establish jurisdiction and begin the preliminary steps of the investigation. Without the TSPs' cooperation, the police would have to seek individual warrants for all IP addresses to obtain this information, causing unnecessary delays in time-sensitive investigations.

- **Child Porn on the Internet – Real -Time Activities**

To identify suspected child pornographers who are using public computers in real-time to conduct their activities, police must obtain their names and addresses before the suspects leave the public computer terminals. TSPs are presently not compelled to give this information without a warrant, and for obvious reasons, a warrant would be impractical in these situations due to the time-sensitive nature of the investigations.

- **Death Threats – via E-mails/On-line Forums**

Death threats are often uttered over the Internet via e-mail messages or on-line forums. While police are sometimes aware of a suspect's e-mail or IP address in these situations, they require TSPs assistance in providing the suspect's name and address. Police may not have time to obtain a warrant in these situations.

- **Contacts of Individual Under Warrant**

When police and CSIS have been authorized by a court to intercept private communications, such as a suspect's or target's e-mail messages, investigators will know the subject of the interception authorization. If another person communicating with the suspect or target becomes a suspect in the investigation, and police want to obtain a court's authorization to intercept that person's communications, they will need to identify the person's name and address to complete the application for the authorization. If the TSP refuses to provide this

information to police without a warrant, the police must take the intermediate step of obtaining a search warrant to obtain the information from the TSP, during which valuable time and potential evidence may be lost.

- **Human Trafficking**

Illegal migrants who enter Canada often destroy their travel documents before entering Canada. Upon their search by immigration officials, they are often found to be in possession of a Canadian phone number belonging to a contact in an international smuggling ring that will aid them in the next step of their journey. The cooperation of TSPs is important in helping to identify the name and address of the subscriber associated with the telephone number. A warrant is impractical in these cases as human traffickers will often quickly dispose of a phone if the illegal immigrants do not make contact within a certain period of time.

- **911 Hang up calls**

Police across Canada receive 911 hang up calls on a regular basis. A person telephones the police to request assistance from them and either hangs up or are forced to hang up for some unknown reason. The police must have access to the name and address of the telephone subscriber in order to respond to these calls for assistance.

- **Abduction / Kidnapping**

In these cases the abductor or kidnapper will inevitably make calls to persons known to him/her. Immediate access to the subscriber information associated with the abductor or kidnapper's telephone number is vital for police to be able to locate him/her.

- **Runaway Children**

In cases where runaway children contact their parents via e-mail or cellular telephone without identifying their location, police need the subscriber information associated with the e-mail or cellular telephone to be able to determine where the children are. If police have to obtain a warrant to obtain subscriber information for this purpose, valuable time is lost in the investigation.

- **Dialed Number Recorders**

Currently, while police obtain court authorizations to utilize dialed number recorders, TSPs still insist that a warrant for the subscriber information associated with the dialed numbers also be obtained. While police engage in the process of obtaining a secondary authorization to obtain basic subscriber information for this purpose, valuable time and potential evidence is lost.

- **Subscriber Identity Modules (SIMs)**

Subscriber Identity Modules (SIMs) are useful to police as they assist in identifying the owners of particular cellular telephones or other devices. Police may obtain SIMs further to the execution of a search warrant, for example. TSPs' assistance is then required to provide the subscriber information associated with these modules. Currently, some TSPs refuse to provide this information without a court warrant. While police engage in the process of obtaining basic subscriber information for this purpose, valuable time and potential evidence is lost.

Refusal by TSPs to Disclose Customer CNA

Percentage of Total Refusals – Statistical Collection Issues

The question of how frequently TSPs refuse to provide CNA to law enforcement on a voluntary basis is difficult (if not impossible) to quantifiably measure, given current statistical gathering tools. Presently, there is no nation-wide statistics gathering tool that collects data on the refusal rates of CNA requests.

Inquiries to the RCMP have revealed that in order to collect such data, a national dispatch would have to be issued to all law enforcement agencies and an administrative system to collect and measure the accuracy of the statistical evidence collected, would have to be put in place. Needless to say this would involve a huge undertaking and would require agreement at senior levels.

In Canada, the formal gathering of criminal justice statistics is done by Statistics Canada's Canadian Centre for Justice Statistics (CCJS), in co-operation with the policing community. These statistics are gathered through the Uniform Crime Reporting survey (UCR). The UCR survey is designed to measure the incidence of crime in Canadian society and its characteristics. However, the UCR data is primarily focused on the "charging stage" of investigations.

Investigative activities, such as the number of times a TSP refuses to provide CNA is, therefore, are not captured in the UCR.

In the absence of clear requirements on TSPs to provide CNA information, [redacted] With this kind of behaviour in the field, even an anecdotal survey would not produce useful statistics on rates of refusal by request. A survey might be done on the number of TSPs that either do or do not provide

CNA, and in what circumstances (e.g., for child pornography investigations, but not for others).

The only statistics that are available on the percentage of refusals for CNA requests are those collected by the National Child Exploitation Coordination Centre (NCECC). However, these statistics are not representative of CNA refusals in general; rather, they represent a small sub-set of refusals dealing exclusively with instances of child exploitation over the Internet. The information cannot therefore be generalized.

NCECC statistics on child exploitation-related refusals of CNA

- NCECC investigators make approx. 200 requests a month for CNA information from Internet service providers (ISPs).
- On average, 35% of requests to ISPs are refused or the information has been purged.
- In May 2007, 44% of requests for CNA were unsuccessful (425 requests sent; 187 refusals)
- In cases of refusal, leads are concluded without an investigation.
- Reasons given for refusal are reported as: lack of data retention; disclosure prohibited by PIPEDA; mistaken belief that the NCECC is "fishing" rather than investigating; demand for evidence of "lawful authority" and demands for warrants where none are possible nor required.
- NCECC investigators calculate that they spend approx. 25hrs/week in conversation with ISP legal counsel attempting to convince them of their ability to voluntarily assist.

Grounds for Refusals

The primary rationale given by TSPs for refusing to provide CNA information to the police on a voluntary basis is concern for liability issues. Faced with ambiguity in the law, some TSPs choose to proceed with caution and demand a warrant before any information will be provided.

However, the question of liability is laid bare in cases involving child exploitation over the Internet. Many ISPs have made a strategic calculation as to where the greater risk lies. Harm to a child and associated public outcry is the only scenario that often outweighs the risk of liability from customer dissatisfaction or litigation.

Even when they might not otherwise share such information, many ISPs have agreed to do so under the auspices of the Canadian Coalition against Internet Child Exploitation (CCAICE). The CCAICE is a partnership between ISPs and police, in which ISPs agree to voluntarily provide CNA in cases relating to child exploitation over the Internet. One of the most significant projects undertaken by the CCAICE was the standardization of a template to request CNA information from an IP address. The template has been refined and is reported to be a success by police and CCAICE members. In cases involving suspected child exploitation over the Internet, most major ISPs will provide CNA information to investigators when the approved template is used. However, it is important to note that not all ISPs in Canada are members of CCAICE and participate in this voluntary initiative.

This template process has the following limitations: ISPs may withdraw their participation at any time; there are no obligatory time frames for response; ISP personnel changes may impact cooperation; after hours requests for information are not acted upon in a timely manner; some ISPs provide insufficient information (city only) which then requires a duplicate request from the police of jurisdiction; if the police are from one province and the customer is from another, the ISP may request "local" police to make the request; some ISPs will not verify the information provided; there are demands for unnecessary production orders and demands for warrants for information which do not require one nor would support one, and in some cases simply refuse to assist. One ISP even advertises that it will delete a customer's account in the event of a "personal emergency", which likely refers to police interest.

Who Refuses

No data exist as to the number of TSPs that refuse to voluntarily disclose CNA information to law enforcement.

At least one provider [redacted] has stated that they will not voluntarily comply with any CNA requests from law enforcement, no matter what the circumstances. Other providers will comply on a case-by-case basis, depending on various factors, including: the nature of the request, the relationship with the law enforcement agency making the request, the personnel working at the time, etc.

Many TSPs have acknowledged the relatively benign nature of the information being sought. Extensive consultations with industry would suggest that most TSPs are willing to comply with CNA requests without a warrant, if the legislative framework were to make this obligation clear. As such, it is expected

that this aspect of the proposed lawful access legislation would be supported by the majority of TSPs – as it would provide clarity and address TSP liability concerns.

Other Considerations – Expectation of Privacy

It should be emphasized that the information obtained under a CNA request (including: name, address, telephone number, email addresses and IP address) generally carries a low expectation of privacy.

CNA information can be compared to a return address on an envelope – not the contents of the letter. As such, the current level of effort expended by police to receive minor information is a major impediment to effective law enforcement.

Finally, it should be noted that if the proposals related the CNA information are approved, it would establish a record keeping obligation for law enforcement using the proposed administrative regime. It is anticipated that statistics on the use of CNA information could be gathered and form part of the proposed five-year parliamentary review of the legislation.

Utility of CNA Requests

Consultations with the RCMP and Canadian Association of Chiefs of Police (CACP) have indicated that this information is used frequently and is extremely valuable across a range of investigations and activities. The utility of this information to police investigations and general policing duties cannot be overstated as this information permits law enforcement to:

- clear an individual from an investigation or lay charges;
- seek a judicial warrant for further investigation (often the information will be used to prepare a warrant for a residential search or search of the ISP's records); and
- undertake additional investigative techniques, such as surveillance or other types of investigative inquiries

Pages 423 to / à 456

are not relevant

sont non pertinentes

Public Safety Canada | Sécurité publique Canada

Assistant Deputy Minister | Sous-ministre adjoint

Ottawa, Canada
K1A 0P8

SECRET CC

Seen by the DM
Vu par le SM
MAR 22 2011

DATE: MAR 18 2011

File No.: 6950-1 / 376447

MEMORANDUM FOR THE DEPUTY MINISTER

Lynda,
We need to discuss recent letter I received from Jennifer.
B.

PRIVACY COMMISSIONER'S CONCERNS WITH LAWFUL ACCESS LEGISLATION

(Information Only)

ISSUE

During your meeting with Ms. Jennifer Stoddart, Privacy Commissioner of Canada, on December 15, 2010, privacy issues related to Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act*, were discussed and Public Safety (PS) committed to reviewing Ms. Stoddart's concerns and suggestions.

BACKGROUND

During the meeting, Ms. Stoddart reiterated concerns with allowing police, the Canadian Security Intelligence Service (CSIS) and the Competition Bureau to obtain basic subscriber information without a warrant for any investigations. She suggested that additional privacy risk mitigation measures should be included in the proposed legislation, such as:

- establishing a 'serious crime' threshold below which authorities would be required to seek a warrant to request basic subscriber information;
- introducing strengthened internal accountability practices, such as requiring that senior officers review and approve all requests for basic subscriber information; and
- amending section 20(1) of Bill C-52 to require annual, rather than 'regular', internal audits of the practices that ensure compliance with the safeguards established under the basic subscriber regime.

The Privacy Commissioner also asked PS to clarify the relationship between Bill C-52 and Bill C-29 (*Safeguarding Canadians' Personal Information Act*), which proposes amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Finally, she requested clarifications regarding the function and purpose of s.20(6) of Bill C-52, which requires that the federal Privacy Commissioner annually report on the role and powers of provincial public officers responsible for privacy.

SECRET CC

s.21(1)(a)
s.23

CURRENT STATUS

Threshold for serious crime

[redacted]

[redacted]

[redacted]

Not relevant

[redacted]

.../4

Not relevant

[redacted]

Annual audits

Ms. Stoddart's final recommendation was that PS consider amending s.20(1) of Bill C-52 to require annual, rather than regular, internal audits of the practices that ensure compliance with the safeguards established under the basic subscriber regime. While this would result in an increased administrative burden on authorities, it would arguably bring more clarity and structure to the audit process.

[redacted]

Points of clarification

Not relevant

With respect to the relationship between Bill C-52 and the *Safeguarding Canadians' Personal Information Act* (Bill C-29), Bill C-29 expands the number of circumstances in

.../4

which personal information can be collected, used or disclosed without consent, upon request and under lawful authority. The Bill clarifies that the concept of lawful authority is not tied to subpoenas or warrants; rather, it includes a more general authority. This more clearly allows the disclosure of personal information without consent to authorities on this expanded basis. While this might reduce the frequency of service providers refusing to provide basic subscriber information without a warrant, Bill C-29 will not actually compel them to supply this information.

Bill C-29 will apply the existing process in law for a service provider to first consult with and obtain permission from the agency that requested subscriber information, before notifying a subscriber that the service provider has released that subscriber's information to that agency. This serves to protect the integrity of investigations.

Finally, the Privacy Commissioner has two functions under s.20(6) of Bill C-52. First, she must identify, on an annual basis, the provincial public officers who will receive the reports summarizing the audits that provincial and municipal police forces conduct on their subscriber information practices. Second, she must report on the powers of these provincial public officers to conduct external audits on the controls and practices that provincial and municipal police forces have implemented for the subscriber information regime. This function serves to identify any legal or resource deficiencies that could impede the ability of provincial authorities to adequately audit the subscriber information regime.

NEXT STEPS

PS officials will offer to meet with the Privacy Commissioner's staff to again provide clarification on the points raised at the December 15, 2010, meeting and to explain the privacy safeguards in Bill C-52. PS officials will also further assess the merits and obstacles associated with the potential amendments outlined above and prepare advice in advance of discussions during the Parliamentary Committee review of Bill C-52.

Should you require additional information, please do not hesitate to contact me at (613) 990-4976 or Michael MacDonald, Director General, National Security Operations, at (613) 993-4595.

for Lynda Clairmont
Assistant Deputy Minister
Emergency Management and National Security

Prepared by: Maciek Hawrylak
Julie Thompson

ANNEX A
LAW ENFORCEMENT REQUESTS TO TSPs FOR SUBSCRIBER INFORMATION: SELECTED EXAMPLES

Not relevant

[redacted]

Following the enactment of PIPEDA (the *Personal Information Protection and Electronic Documents Act*), some TSPs began to question the "lawful authority" of police to obtain this information voluntarily from them. These TSPs indicated that they would not release such personal information unless police have a warrant or court order to compel the TSP to provide it. The proposed new statutory requirement, obliging a TSP to provide this information to police after a proper request has been made, should end the TSPs' uncertainty related to the "lawful authority" of police to obtain this information without a warrant.

People who are not familiar with day-to-day policing functions, both investigative and general policing duties, cannot readily appreciate why police need to obtain customer name, address and some other basic identifying information, such as an IP address or SMTP email address, without a warrant or other court order. At public consultations on lawful access legislative proposals, held in February and March 2005, civil society and privacy advocates expressed serious apprehensions about police having the power to obtain certain basic subscriber information without judicial or other independent oversight.

To illustrate why police need to obtain TSP customers' names, addresses and certain other basic identifying information without first obtaining a warrant or another court order, the following examples have been compiled. These examples are based on real experiences. They are presented in two sections: the first one describes situations where obtaining a court order is simply not an option and the second one describes situations where it would be possible to seek a court order but, under the circumstances, it would not be practical or effective to do so. Preceding these examples is a brief summary of the steps and time involved in seeking a search warrant.

1. The Steps to Obtain a Warrant

The investigator must explain in writing, his or her credentials as a peace officer, the history of the investigation, how the investigator came into possession of the phone number or email address or other subscriber information, the criminal offence which is being committed and how the elements of the offence have been proven. Writing up this explanation of the investigation to date can take any where from three to five hours . Once these criteria have been documented, the investigator's supervisor must review and sign off on the warrant request (information to obtain). The warrant request is then reviewed by the appropriate judicial authority. The judicial authority review process can involve driving to where the Justice of the Peace resides and waking up the Justice in the middle of the night for review. It could also involve using a Justice of the Peace Service Centre (this is the system that is used in the Greater Vancouver area of BC). The Justice of the Peace Service Centre is a central repository for all warrant requests after hours. The requests are received via fax and reviewed according to time of receipt and priority. The review process can take any where from one to three hours depending on how busy the Justice or Centre is and how many questions the Justice has upon review. The warrant is then signed and turned over or faxed to the investigator and it can then be executed.

2. Examples Where Court Orders to Obtain Name, Address or Similar Information **Are Not An Option**

2(3) Informants will often volunteer to police the names and phone numbers of people involved in criminal activity, such as drug trafficking. An informant will usually only know a first name or a nickname and an associated phone number and the type of criminal activity the person is allegedly involved in. A first name and a telephone number is not enough information to obtain a warrant or even to start an investigation. However, a phone number may be used to build an investigation, at its very early stages. Checking a phone number provided by an informant against a TSP's information regarding the customer name associated with that number is invaluable to police in these instances. Police can then corroborate or refute the informant's information, which can provide or conclude an investigational lead.

2(4) A police officer performing general duties, such as patrol in rural settings, may draw upon subscriber records to obtain an accurate civic address in a relatively secure manner. In small towns or rural areas, post office box or a rural route numbers are often used as the address information for identification documents, such as drivers' licences and vehicle registrations. But these addresses are not sufficient in a situation where an officer must determine a civic address, for example to notify next of kin after a serious or fatal motor vehicle accident. Telephone subscriber records will usually include civic addresses as well as mailing (P.O. Box or R. R. #) addresses. Therefore, by providing the individual's name and mailing address to a TSP, police are able to establish that person's civic address.

2(5) Many people do not carry their wallets or identification when walking the dog, running errands in their neighbourhood, going for a hike, bike ride, walk, or canoe trip. However, usually they will carry their cellular phones, for emergencies and so that family members and friends can reach them. Police are often called upon to assist emergency health services in cases where an incapacitated person cannot be identified. If such a person was not carrying any identification, but was carrying a cell phone, then the information taken from the phone, with the assistance of the TSP, can be used to identify the person. For example, if the person's phone is still operating and not locked, police can obtain the phone number off the phone. If the phone was damaged or is not operating for other reasons, then police may be able to draw from the device, depending on its type, either an electronic serial number (ESN), international mobile equipment identity (IMEI) or international mobile subscriber identity (IMSI). With the cell phone number or these other identity numbers, which are unique to a subscriber's phone, police can approach the TSP to obtain information as to the name and address of the subscriber (who is presumably the unidentified person or someone who knows the unidentified person).

2(6) Crisis lines, for example suicide prevention lines and child abuse help lines, receive calls for help from people who are threatening to hurt themselves or from people who are being abused. Crisis lines may subscribe to caller ID and, in certain cases, they may need to relay the nature of the crisis as well as the caller ID to the police for assistance. The name and telephone number displayed for a caller in distress can be checked against a TSP's customer name and address records and used to help locate the caller, to try to prevent them from hurting themselves or to take steps to protect a victim from being subjected to further abuse. While suicide and threats of suicide are not criminal offences, the police have a duty to assist the person under provincial / territorial mental health laws or similar protective legislation. However, police cannot use a search warrant in this type of situation to obtain the caller's address information.

2(7) If a child does not return home from school by a certain time, his concerned parents may first check with the school to try to locate the child. Once the school confirms that the child left at the usual time, his concerned parents may then call the child's friends, as well as their neighbours. After several hours, as evening and darkness closes in, the parents may turn to other sources to locate their child, for example, checking the child's email on the home computer they could discover the child had arranged to meet "Buddy" (not a name known to them) at "the usual spot" after school. If the parents have not contacted police by this point, likely the email will prompt them to now seek help from the police. However, without additional information and reason to believe foul play, police would only be able to consider the child missing at this stage. They would not have sufficient grounds to obtain a warrant to compel the Internet Service Provider to disclose the full name and civic address of "Buddy". If police contact the ISP with the SMTP email address of "Buddy", as well as his IP address at the date and time of the email communication, a cooperative ISP, realizing the missing child could be in serious danger, would probably set aside concerns about disclosing customer information without a warrant and provide police with the name and address of "Buddy". Unfortunately, some ISPs, who are not experienced dealing with these types of time-sensitive emergencies, and who are concerned about protecting their customer's privacy, currently can refuse to provide this information to the police.

2(8) In Canada, all international online child sexual exploitation tips go through the National Child Exploitation Coordination Centre (NCECC), which is mandated by the Government of Canada to combat the sexual exploitation of children on the Internet. Currently the NCECC receives approximately 600 international tips per year and that number is rising. The types of tips the NCECC receives are quite varied. For example, in relation to luring cases a tip could involve anything from simply a nickname (my daughter just had some creep named Eddie44 try to meet her in a park for sex) to a chatline with date and time or a chat with nickname and IP address and date and time. In many cases the tips do not provide sufficient information in themselves to form the basis to obtain a warrant.

Some recent tips have consisted of information found on "profiles" that people have set up. (A profile is registration information which a user enters to allow the user access to webmail email, instant messaging, chat or other online services.) For instance on a profile for Yahoo, MSN, America Online or another web portal offering online services to subscribers, a person might post child porn pictures or indicate they would like to find others to have sex with their children. In these cases as well, the tip could consist of a nickname or username only. It would be important, in this situation for the NCECC to be able to give the username to the ISP (for example Yahoo, MSN or America Online) and in exchange the ISP could provide to the NCECC the IP address and date and time that the person registered the profile.[4]

Procedurally, after receiving a tip, the NCECC will next ensure that the tip relates to activities that constitute an offence in Canadian law and gather any information that may further substantiate the tip. This step could involve reviewing intelligence or databases, such as CPIC, to see if this information has been received from other sources or if that nickname had previously been noted. The next step for the NCECC is to send the tip and other relevant information it has gathered in relation to the tip to the police force of jurisdiction for investigation. However, to send this information to the proper police jurisdiction the NCECC needs to obtain, at a minimum, the location of the IP address. Without that information, the NCECC is unable to identify the police force of jurisdiction. The NCECC could arbitrarily send the tip to any police force; however, a police service would probably be quite reluctant to work on the tip if the suspect may very well not be in its jurisdiction, as it would not be effective use of limited police resources. Valuable time would also be lost if the tip were sent to the wrong jurisdiction for investigation. The loss of time could be very damaging in that children may be sexually exploited during this period and the longer that the investigation is delayed, the greater the chances that the ISP logs or data will be overwritten or deleted and potential evidence would be lost and never be obtainable under warrant.

2(9) When police recover stolen property, such as a television or computer, if they are able to identify the name and address of the owner of the property they may contact the owner to return the property. However, if several months have passed since the time the property was reported stolen and the time it was recovered, the owner may have changed residences and police may no longer have a current address for the owner. Although a **Not relevant**

[4] Author's Note:

quick and reliable way to check the current address of the owner would be to inquire with a local telephone service provider, the TSP may feel it is not at liberty to disclose the customer's address, which is personal information, under PIPEDA (the *Personal Information Protection and Electronic Documents Act*). The TSP might tell the police it will only disclose this information pursuant to a warrant. However, police would not be able to seek a warrant to obtain current address information to return stolen property, since the address would be needed simply for the purposes of returning the stolen item and not for the purposes of an investigation.

3. Examples Where Court Orders to Obtain Name, Address or Similar Information **Are Not Practical**

3(1) People will often use nicknames or pseudonyms when using the online (Internet-based) chat programs, especially if the person is involved in criminal activities such as the distribution of child pornography or child luring). Chat sessions take place in real time and the only information that can be captured, aside from the date and time, is the suspect's nickname and Internet Protocol (IP) address. Suspects will further try to conceal their identity and location by using a computer terminal that does not belong to them, such as a terminal at an Internet café, library, or recreation centre. In such a case, if the suspect is not caught behind the keyboard, it would be very difficult to locate the person who engaged in the chat session. In order to catch the suspect before he or she leaves the chat session, the investigator must have immediate access via an ISP to the Internet customer's name and street address associated with the IP address, date and time of the chat.

3(2) In a recent NCECC project, the NCECC was given a list of 2000 Canadian targets who had bought child pornography online. The target information included the IP address and date and time of the purchases. The NCECC first needed to determine which police force had jurisdiction to investigate the offences. Without getting the jurisdiction information (i.e., the jurisdiction of the online purchaser) from the ISPs 2000 warrants would have had to be processed simply to obtain that information. The NCECC was able to obtain this information voluntarily from cooperative ISPs. It then distributed the target information to police forces of jurisdiction, resulting in some police agencies receiving 200 or more targets to investigate.

When police agencies receive information on 200 or more suspected purchasers of child pornography, they need to be able to prioritize their investigative files, so that those suspects with a history of sexual assault, on probation, having access to children or those convicted of producing child pornography are given the highest priority. The best way to set priorities is to get the customer name and address information from ISPs, which is associated with the IP address and date and time of the online child porn purchase, and to cross reference those names with CPIC and other relevant databases to ensure that, if the customer name and address information matches with known child predators then these targets will be investigated as top priorities.

[redacted]

[redacted]

3(4) With the proliferation of computers and email, uttering anonymous threats via email, is becoming common. From such an email, police can determine the email address, IP address and date and time of the email. In a case where a suspect threatens to hurt or kill the receiver of the email, Internet Service Provider records of the IP address and email address at the date and time of the threat could identify the name and address of an otherwise unknown suspect. The nature of the threat will dictate whether or not the police could obtain a warrant for this information. For example, if a suspect threatens to hurt or kill an individual within a matter of hours, there may not be time to obtain a warrant.

3(5) Students sometimes make death threats against other students or teachers on Internet bulletin board services or Internet posting forums. In order for police to properly protect these students or teachers the threats made against them on bulletin boards or posting forums must be investigated. The time, within which the police must try to establish the bulletin board poster's identity, is extremely critical. The time to act is too limited for the police to use warrants to obtain the information they need, since the threats are usually posted only minutes or hours before a true threat materializes. As a result, police would draw upon the bulletin board posting to determine the date and time of the posting, as well as the related IP address. Police would then approach an ISP with this particular information and seek to establish to whom the IP address is registered. The IP address registration information would bring police one step closer to being able to identify the likely source of the posting, to make a risk assessment of the potential threat, and to determine the most suitable response.

[redacted]

[redacted]

3(8) The vast majority of migrants attempting to enter Canada illegally do so via criminal organizations that have established smuggling routes and proven practices to circumvent immigration controls. The migrants are normally provided with documents and explicit instructions on how the smuggling operation will take place, who their "escort" will be, what they are to say to immigration and airline officials throughout the journey, and how to contact the Canadian "link" in the smuggling operation once they arrive at the airport in Canada. In most cases, migrants attempting to illegally enter Canada via a commercial flight will either destroy their travel and identity documents before landing in Canada or turn the documents over to the "escort" who has accompanied them on the flight. Upon arrival in Canada they immediately claim they are refugees and are referred to the Citizenship and Immigration Canada (CIC) office at the airport. During the screening process by Immigration officials, these migrants and their accompanying luggage are routinely searched. Often, Immigration officials find these migrants in possession of a Canadian phone number, sometimes accompanied by a first name. In these cases the RCMP may be contacted to pursue a criminal investigation involving a suspected smuggling operation.

If they are not truly refugees, the Canadian phone number they carry is usually the contact number they have been instructed to call once they have been processed and released by Immigration at the airport. In other words, it is the number for the Canadian connection in an international people smuggling ring who is waiting to pick them up from the airport. The migrants may be smuggled next into the US or they may be helped to disappear into the underground world of illegal immigrants. In this situation, the RCMP have a small window of opportunity to try to determine the link between the number found on the refugee claimant at the airport and the smugglers who may be standing by to whisk the person away from the airport. For example, when the RCMP provides such a phone number to a TSP, if the TSP is able to quickly identify the name and civic address associated to the number, the RCMP can then look into whether the name or address

information points to a known or suspected person involved in smuggling people into Canada. Obtaining this information quickly may make it possible to apprehend the smuggler while still in the process of moving the operation's human cargo. But if the name and address information associated with the phone number can only be obtained with a warrant, which currently is sometimes the case, critical investigative time will be lost and the trail leading to the smugglers involved in this international conspiracy could go cold.