SUMMARY Allocation of Funding

	2011-12				2012-13				2013-14				2014-15				2015-16				Ongoing			
	FTE	Salaries	O&M	Total	FTE	Salaries	O&M	Total	FTE	Salaries	O&M	Total	FTE	Salaries	O&M	Total	FTE	Salaries	O&M	Total	FTE	Salaries	O&M	Total
Direct Costs:																								
CMB	1.00	53,711	165,693	**219,404**	1.00	53,711	80,075	**133,786**	1.00	53,711	66,647	**120,358**	1.00	53,711	66,647	**120,358**	1.00	53,711	66,647	**120,358**	1.00	53,711	66,647	**120,358**
IT			31,975	**31,975**			36,197	**36,197**			33,444	**33,444**			33,444	**33,444**			33,444	**33,444**	0.00	-	33,444	**33,444**
Accomodations	1.00	53,711	133,718	**187,429**	1.00	53,711	43,878	**97,589**	1.00	53,711	33,203	**86,914**	1.00	53,711	33,203	**86,914**	1.00	53,711	33,203	**86,914**	1.00	53,711	33,203	**86,914**
HR			-	**-**			-	**-**			-	**-**			-	**-**			-	**-**	0.00	-	-	**-**
ADM			-	**-**			-	**-**			-	**-**			-	**-**			-	**-**	0.00	-	-	**-**
EMNS	7.00	618,283	282,406	**900,689**	10.00	876,178	230,773	**1,106,951**	11.00	956,086	183,310	**1,139,396**	12.00	1,035,994	217,386	**1,253,380**	12.00	1,035,994	202,884	**1,238,878**	12.00	1,035,994	202,884	**1,238,878**
LPB	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**
CSP	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**
SPB	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**
IGCSIS	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**
Comms	0.50	44,301	87,494	**131,795**	0.50	44,301	2,494	**46,795**	0.50	44,301	52,494	**96,795**	0.50	44,301	52,494	**96,795**	0.50	44,301	2,494	**46,795**	0.50	44,301	2,494	**46,795**
Audit	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**
Legal	0.00	-	206,344	**206,344**	0.00	-	300,705	**300,705**	1.00	53,711	305,691	**359,402**	1.00	53,711	355,691	**409,402**	1.00	53,711	305,691	**359,402**	1.00	53,711	305,691	**359,402**
OGD	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**
Total Direct Costs	**8.50**	**716,295**	**741,937**	**1,458,232**	**11.50**	**974,190**	**614,047**	**1,588,237**	**13.50**	**1,107,809**	**608,142**	**1,715,951**	**14.50**	**1,187,717**	**692,218**	**1,879,935**	**14.50**	**1,187,717**	**577,716**	**1,765,433**	**14.50**	**1,187,717**	**577,716**	**1,765,433**
Standard Costs:																								
CMB	0.77	48,121	200,163	**248,284**	1.04	65,106	137,222	**202,328**	1.22	76,428	134,295	**210,723**	1.31	82,090	128,118	**210,208**	1.31	82,090	112,620	**194,710**	1.31	82,090	112,620	**194,710**
IT			68,181	**68,181**			65,334	**65,334**			71,879	**71,879**			73,568	**73,568**			70,402	**70,402**			70,402	**70,402**
Accomodations			125,131	**125,131**			62,619	**62,619**			51,535	**51,535**			42,863	**42,863**			30,531	**30,531**			30,531	**30,531**
HR			4,250	**4,250**			5,750	**5,750**			6,750	**6,750**			7,250	**7,250**			7,250	**7,250**			7,250	**7,250**
ADM [1]	0.77	48,121	2,601	**50,722**	1.04	65,106	3,519	**68,625**	1.22	76,428	4,131	**80,559**	1.31	82,090	4,437	**86,527**	1.31	82,090	4,437	**86,527**	1.31	82,090	4,437	**86,527**
SPB	0.31	24,307	8,232	**32,539**	0.43	32,885	11,189	**44,074**	0.50	38,605	12,776	**51,381**	0.54	41,465	13,701	**55,166**	0.54	41,465	13,701	**55,166**	0.54	41,465	13,701	**55,166**
Comms	0.20	17,172	664	**17,836**	0.26	23,233	899	**24,132**	0.31	27,273	1,056	**28,329**	0.33	29,294	1,134	**30,428**	0.33	29,294	1,134	**30,428**	0.33	29,294	1,134	**30,428**
Audit			7,163	**7,163**			9,742	**9,742**			11,078	**11,078**			11,877	**11,877**			11,877	**11,877**			11,877	**11,877**
Legal			-	**-**			-	**-**			-	**-**			-	**-**			-	**-**			-	**-**
Total Standard Costs	**1.28**	**89,600**	**216,222**	**305,822**	**1.73**	**121,224**	**159,052**	**280,276**	**2.03**	**142,306**	**159,205**	**301,511**	**2.18**	**152,849**	**154,830**	**307,679**	**2.18**	**152,849**	**139,332**	**292,181**	**2.18**	**152,849**	**139,332**	**292,181**
Total of all Costs	**9.78**	**805,895**	**958,159**	**1,764,054**	**13.23**	**1,095,414**	**773,099**	**1,868,513**	**15.53**	**1,250,115**	**767,347**	**2,017,462**	**16.68**	**1,340,566**	**847,048**	**2,187,614**	**16.68**	**1,340,566**	**717,048**	**2,057,614**	**16.68**	**1,340,566**	**717,048**	**2,057,614**

Notes:

[1] Includes CMB's portion of the following Corporate Support Costs: Cost for Corporate Support Staff, Transport and Communication and Other Standard Costs. These costs are allocated to the ADM and will be reallocated to fund pressures.

SUMMARY Allocation by Branch

	2011-12				2012-13				2013-14				2014-15				2015-16				Ongoing			
	FTE	Salaries	O&M	Total	FTE	Salaries	O&M	Total	FTE	Salaries	O&M	Total	FTE	Salaries	O&M	Total	FTE	Salaries	O&M	Total	FTE	Salaries	O&M	Total
CMB	1.77	101,832	365,856	**467,688**	2.04	118,817	217,297	**336,114**	2.22	130,139	200,942	**331,081**	2.31	135,801	194,765	**330,566**	2.31	135,801	179,267	**315,068**	2.31	135,801	179,267	**315,068**
IT	0.00	-	100,156	**100,156**	0.00	-	101,531	**101,531**	0.00	-	105,323	**105,323**	0.00	-	107,012	**107,012**	0.00	-	103,846	**103,846**	0.00	-	103,846	**103,846**
Accomodations	1.00	53,711	258,849	**312,560**	1.00	53,711	106,497	**160,208**	1.00	53,711	84,738	**138,449**	1.00	53,711	76,066	**129,777**	1.00	53,711	63,734	**117,445**	1.00	53,711	63,734	**117,445**
HR	0.00	-	4,250	**4,250**	0.00	-	5,750	**5,750**	0.00	-	6,750	**6,750**	0.00	-	7,250	**7,250**	0.00	-	7,250	**7,250**	0.00	-	7,250	**7,250**
ADM	0.77	48,121	2,601	**50,722**	1.04	65,106	3,519	**68,625**	1.22	76,428	4,131	**80,559**	1.31	82,090	4,437	**86,527**	1.31	82,090	4,437	**86,527**	1.31	82,090	4,437	**86,527**
EMNS	7.00	618,283	282,406	**900,689**	10.00	876,178	230,773	**1,106,951**	11.00	956,086	183,310	**1,139,396**	12.00	1,035,994	217,386	**1,253,380**	12.00	1,035,994	202,884	**1,238,878**	12.00	1,035,994	202,884	**1,238,878**
LPB	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**
CSP	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**
SPB	0.31	24,307	8,232	**32,539**	0.43	32,885	11,189	**44,074**	0.50	38,605	12,776	**51,381**	0.54	41,465	13,701	**55,166**	0.54	41,465	13,701	**55,166**	0.54	41,465	13,701	**55,166**
IGCSIS	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**
Comms	0.70	61,473	88,158	**149,631**	0.76	67,534	3,393	**70,927**	0.81	71,574	53,550	**125,124**	0.83	73,595	53,628	**127,223**	0.83	73,595	3,628	**77,223**	0.83	73,595	3,628	**77,223**
Audit	0.00	-	7,163	**7,163**	0.00	-	9,742	**9,742**	0.00	-	11,078	**11,078**	0.00	-	11,877	**11,877**	0.00	-	11,877	**11,877**	0.00	-	11,877	**11,877**
Legal	0.00	-	206,344	**206,344**	0.00	-	300,705	**300,705**	1.00	53,711	305,691	**359,402**	1.00	53,711	355,691	**409,402**	1.00	53,711	305,691	**359,402**	1.00	53,711	305,691	**359,402**
OGD	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**	0.00	-	-	**-**
Total of all Costs	**9.78**	**805,895**	**958,159**	**1,764,054**	**13.23**	**1,095,414**	**773,099**	**1,868,513**	**15.53**	**1,250,115**	**767,347**	**2,017,462**	**16.68**	**1,340,566**	**847,048**	**2,187,614**	**16.68**	**1,340,566**	**717,048**	**2,057,614**	**16.68**	**1,340,566**	**717,048**	**2,057,614**

EBP				161,179				219,083				250,023				268,113				268,113				**268,113**
Accommodation				104,766				142,404				162,515				174,273				174,273				**174,273**
Grand Total				**2,029,999**				**2,230,000**				**2,430,000**				**2,630,000**				**2,500,000**				**2,500,000**

Bill C-51 - Minister of Justice

An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act which can be referred to as the *Investigative Powers for the 21st Century Act*

Introduced November 1, 2010.

Bill Narrative / Descriptor:

The bill proposes to amend the *Criminal Code* to ensure that law enforcement officials have the authority and ability to fight crime in the current computer and telecommunications environment by updating certain existing offences as well as by creating new investigative powers. This includes specific provisions to obtain the routing data related to a telecommunication or to a service provider involved in the transmission of such a telecommunication, the possibility for police to preserve data, and it enhances the privacy protections with respect to the tracking of the location of a person, as opposed to when a vehicle or thing is tracked. The legislation would clarify that no information shall be disclosed to the police without a judicial authorization.

The proposed legislative amendments would also create the legislative framework necessary for Canada to ratify the Council of Europe's Convention on Cybercrime and its Additional Protocol Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems.

Additional Details

The proposed amendments would allow police to obtain "**transmission data."** Transmission data relates to the underlying means of telecommunication used by a suspect to communicate by telephone or Internet. It can provide information on the type, date, time, origin, destination or termination of a communication, but would not include the content of a private communication.

As is currently the case in the *Criminal Code*, a judicial order would be required before police could obtain transmission data. Two different types of orders would permit this – a **warrant** (when the suspect's data is intercepted in real-time) or a **production order** (to obtain stored transmission data from the service providers involved). Judicial authorizations for this type of data may only be obtained when there are "reasonable grounds to suspect" that the data will assist in the investigation of a crime.

To permit law enforcement officers to trace a communication back to the suspect's original service provider. The proposed legislation would allow police to obtain a limited amount of "**transmission data"** for the purposes of identifying all of the service providers involved in the transmission of emails or other communications. This would help trace cybercrime domestically, as well as enhance international cooperation.

The amendments would create a **preservation order** that would require a telecommunication service provider to safeguard and not delete its data related to a specific communication or a subscriber when police believe the data will assist in an investigation. A preservation order is a "quick-freeze" temporary order, and would only be in effect for as long as it takes law enforcement to return with a search warrant or production order to obtain the data.

(This is not **data retention**. The amendments would **not** require custodians of data to collect and store data for a prescribed period of time for **all** subscribers, regardless of whether or not they are subject to an investigation. A preservation order would be restricted to the data that would assist in a specific investigation.)
In light of new technologies, amendments would improve the existing **tracking warrant's** privacy protections with respect to the tracking of the location of people, while continuing to allow for the tracking of objects, including vehicles. The warrant would allow police to remotely activate existing tracking devices that are found in certain types of technologies (cell phones and telematics devices in some cars, e.g. a GPS). Real-time tracking data could be obtained under this warrant, while historical tracking data could be obtained via a production order.
The amendments would update section 342.2 of the *Criminal Code* in two ways: making it illegal to possess a "device" for the purposes of committing the offence of mischief and indicating that computer programs – such as viruses – are now to be considered as "devices." Currently only the actual or attempted mischief created by the spread of a computer virus is punishable.
The proposed amendments to the ***Mutual Legal Assistance in Criminal Matters Act*** would widen the scope of assistance that Canada could provide to its treaty partners in fighting serious crimes, including computer and computer-related crime, at an international level.

Amendments to the ***Competition Act*** would allow the Competition Bureau to better address significant technology-related challenges that affect its ability to obtain evidence, especially for the violations of deceptive marketing practices and false or misleading representation provisions.
The proposed legislative amendments would also create the legislative framework necessary for Canada to ratify the *Council of Europe's Convention on Cybercrime* and the *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems*.

These multilateral treaties, which were signed by Canada in November 2001 and July 2005 respectively, are the only instruments that provide for broad-based international cooperation for the investigation and prosecution of computer-related crimes. Increasing and strengthening the tools available will assist in obtaining evidence to advance criminal investigations and prosecutions. This reflects the recognition that effective and evolving international assistance mechanisms are vital in combating the ever-growing threat of international criminality.

assumptions, for each of the bills and Acts, conducted in accordance with the Treasury Board Guide to Costing?

Investigative Powers for the 21st Century and Ratification of the Council of Europe's Convention on Cybercrime and its Additional Protocol.

Background

Since 2000, through the lawful access initiative, the Government of Canada has been reviewing its lawful access laws, including the *Criminal Code*, to bring them up to date with issues arising from new technologies. Lawful access consists of the lawful interception of communications and the search and seizure of information used by law enforcement and national security agencies to conduct investigations and to gather intelligence.

There are two distinct components that have emerged as a result of the lawful access initiative:

- Public Safety Canada and Industry Canada have primary responsibility for developing new legislation that would compel communication service providers to procure and maintain intercept capable equipment and provide for access to subscriber information;
- Justice Canada has primary responsibility for *Criminal Code* amendments as well as related amendments to other statutes.

The Investigative Powers for the 21st Century (IP21C) initiative pertains to the second component of the lawful access initiative. The proposals contained in the IP21C initiative specifically address the ability to investigate and prosecute cyber-crime and, more broadly, to collect evidence associated with new technologies.

21st Century's Computer and Telecommunications Environment

Emerging and evolving communications technologies clearly benefit Canadian society, however their use for illicit purposes creates significant public safety challenges. In order to improve the safety of Canadians, including children, in the 21st century's computer and telecommunications environment, new investigative powers are required.

Many of today's crimes involve criminals using mobile cell phones or computers to send messages through the Internet using new telecommunications capabilities. Unlike forensic evidence localized at a murder scene, digital evidence is scattered across dozens of devices at locations sometimes in different jurisdictions. Moreover, electronic data can exist along an entire spectrum of permanence, from being very volatile and transient to being stored on long term storage media. Consequently, specialized investigative powers should be designed to obtain digital evidence not only for high-tech computer crimes, but also to deal with everyday offences, when a criminal sends an email or uses their cell phone.

The Legislation

The legislation includes proposed amendments to the *Criminal Code*, the *Mutual Legal Assistance in Criminal Matters Act* and the *Competition Act*. The proposed amendments would provide police with more precise and less cumbersome investigative tools.

In addition to updating certain existing offences that are facilitated by the Internet, including child sexual exploitation, the reforms will create new production and preservation orders to address today's computer and telecommunications environment.

All of the new legislative provisions are necessary in order to meet domestic needs. However, they would also allow Canada to ratify the *Convention* and its *Additional Protocol,* which are the only existing instruments at the international level to combat computer-related crime. Ratification of this *Convention and its Additional Protocol* would also Canada to cooperate with other signatory countries in the investigation of cybercrime and help access evidence that, due to the nature of Internet technology, can actually be found on a different continent.

Overview of Investment

The legislative provisions will have funding implications for Justice Canada, the ODPP, the RCMP, and DFAIT. New resources will be required to support the implementation of the legislative provisions and the ratification of the *Convention* and its *Additional Protocol*. Specifically, new resources will be required for:

- *Criminal Code* and *Mutual Legal Assistance in Criminal Matters Act Amendments*
  - •Legal and Policy Advice and Litigation
  - •Training
  - •Technical Assistance or Investigation
  - •Mutual Legal Assistance and Extradition
- .Ratification of the *Convention* and its *Additional Protocol*
  - •Implementation of the *Convention* and its *Additional Protocol*
  - •International Assistance
  - •Mutual Legal Assistance and Extradition
- Evaluation and Annual Reporting

Listing of Supporting Information / Documentation to Question 4:

See attached annexes
Annex A RCMP
Annex B ODPP
Annex C Justice
Annex D DFAIT

Bill C-50 – Minister of Justice
An Act to amend the Criminal Code (interception of private communications and related warrants and orders) also known as the *Improving Access to Investigative Tools for Serious Crimes Act*
Introduced October 29, 2010
Bill Narrative / Descriptor:
The amendments are designed to streamline the application process when specific court orders or warrants need to be issued in relation to an investigation for which a judge has given a wiretap authorization. In response to recent court decisions in British Columbia and Ontario, amendments are also proposed to section 184.4 of the *Criminal Code*, which provides authority for wiretapping without a warrant in exceptional circumstances, such as a kidnapping or a potential bomb threat. The amendments being proposed would enhance privacy safeguards by adding requirements to notify persons who were intercepted under this provision and to report annually on the number of intercepts being done when private communications are intercepted in these exceptional circumstances. Such requirements already exist in relation to other *Criminal Code* wiretap authorities. (The amendments were previously included in Bill C-31 introduced in the Second Session of the 40th Parliament.) Bill C- 50 would provide law enforcement with access to the technical tools in order to investigate serious crime, including kidnapping and murder. First, it would provide for a single process for obtaining court orders relating to an investigation for which a wiretap authorization was obtained. Under this process the contents of all the applications would be sealed in a single package in order to maintain secrecy for the purpose of not jeopardising and undermining the ongoing investigation. Second, the Bill will create new safeguards for section 184. 4 of the Code to permit the interception of private communications in exceptional circumstances. These safeguards will remedy Charter defects of the current provisions noted by the Courts.
Explanation of any Omissions to the Questions Below:
No detailed cost information is available because there are no costs associated with this bill The bill will ensure that an existing provision (re: wiretaps in exceptional circumstances) fully respects the Charter. The streamlined application process for other court orders should improve investigative powers and not add costs.

What are the incremental cost estimates broken down by Capital, Operations & Maintenance and Other categories?
Not applicable. An explanation has been provided under the heading "Explanation of any Omissions to the Questions below".

What is the baseline departmental funding requirement excluding the impacts of the bills and Acts, broken down by Capital, Operations and Maintenance and Other categories?
Not applicable within the context referred to in the overview document.

What are the total departmental Annual Reference Level (ARL), including all quasi-statutory and non-quasi-statutory items, including Capital, Operations and Maintenance and Other categories, including the incremental cost estimates?
Not applicable. Reference is to be made to the overview document and comments in relation to Annual Reference Levels.

What are the detailed cost accounting, analysis and projections, including assumptions, for each of the bills and Acts, conducted in accordance with the Treasury Board Guide to Costing?
As noted above, no detailed cost information is available because there are no costs associated with this bill. The bill will ensure that an existing provision (re wiretaps in exceptional circumstances) fully respects the Charter. The streamlined application process for other court orders should improve investigative powers and not add costs.

Royal Canadian Mounted Police

A significant part of the IP21C initiative will rely on personnel having a specific expertise hired by the RCMP in due time to respond to the workload pressure once new legislative provisions will come into effect.

The Amendments

The proposed amendments to the *Criminal Code* and the *Mutual Legal Assistance in Criminal Matters Act* (MLACMA) as will impact the RCMP Special "I" program (units in the RCMP that are responsible for electronic surveillance). In particular, the proposed new Transmission Data Warrant (TDW) and MLACMA modifications will result in the need for additional human and financial resources to meet the increased demand from domestic and foreign law enforcement for Special "I" services.

Resource Requirements:

Technological Crime Program:

The RCMP's Technological Crime Program (TCP) has teams located throughout Canada. The TCP does not presently have the capacity to address the requests for assistance and/or conduct the investigations which are anticipated to be forthcoming as a result of these amendments. Delivering on and/or supporting the additional investigations, requests for analysis and/or requests for assistance stemming from the proposed changes at the current resourcing levels will not be possible without a base minimum increase in resources. An increase in offences and scope at this juncture for the TCP must be resourced to ensure that the TCP is able to deliver on the promises and intent of the legislative changes.

By ensuring the RCMP has the capacity to support the proposed changes, the RCMP will be in a position to provide timely and effective response and services to investigations in direct support of the amendments proposed.

The RCMP's TCP has two mandates:

- Investigate pure computer crimes where the computer or the data therein are the target of the offence as opposed to being used to facilitate the offence.
- Provide specialized technical investigative services in all other technologically facilitated crimes (e.g., online fraud).

Front line service delivery pertaining to digital evidence processing as well as the investigations of pure computer crimes are provided through eight Integrated Technological Crime Units (ITCUs) located strategically through out the country as well as through dedicated program areas located within the Technological Crime Branch (TCB).

The TCP provides a number of services which will be impacted by the proposed changes through an increase in:

- demand for forensic analysis of new technologies and related storage device;
- requests for analysis of mobile devices such as cellular phones and Personal Digital Assistants;
- need for acquisition of digital information and/or intelligence through execution of general warrants and covert entries (both computers and mobile devices);
- need for online covert research through the monitoring and recording of Web Sites of interest in support of the new offences or broader definitions of offences;
- requests for consultation with respect to Part VI authorization under the *Criminal Code* and general warrant or Order preparation and information which may be available via digital transmissions, covert penetration of target technologies;
- requests for consultation and dialogue with respect to investigational and operation planning;
- requests for preparation and/or assistance with respect to preservation orders, production orders and other court documents as well as in search preparation and execution where computers are involved;
- requests for technical assistance with interviews involving technically knowledgeable persons;
- preparation of digital evidence for disclosure purposes and presentation to the crown and the courts;
- costs for technological education of members of the TCP;
- need for research, development, verification and validation of new tools, techniques, methodologies and processes relating to new technologies;
- costs for implementation of new tools, techniques, methodologies and processes relating to new technologies;

- a number of investigations of pure technological crimes as the definitions within the *Criminal Code* are broadened to factor in new technologies;
- need to develop standards, policies, coordinate training, provide strategic planning resulting from the broadening of the definitions within the *Criminal Code* to factor in new technologies;
- need to develop standards, policies, coordinate training and provide strategic planning resulting from the proposed changes to the MLACMA;
- need to provide advanced search and seizure of digital evidence from new technologies with open and embedded systems; and
- need to provide increased data analysis and digital data extraction.

Technology plays a major role in crime, more so today than ever before. The use of personal computer/laptops, the internet and handheld devices has exploded at an exponential rate. They have become staples in today's society. As technology evolves, its usage will continue to grow, resulting in further strains on the RCMP TCP's capacity to service both domestic and international requests in an effective and timely manner.

To summarize:

- The proposed legislative amendments contained in IP21C initiative will provide law enforcement with new powers to address crime in the 21st century's computer and telecommunications environment. The proposed Transmission Data Warrant (TDW) will allow for the real time collection of communications transmission data from service providers located in Canada. This new tool will help law enforcement fight against technically savvy criminals who exploit advances in technology to commit crimes with relative impunity.
- To respond to the anticipated impact these amendments will have, the RCMP is requesting resources to cover the costs associated with the anticipated increase in human and technical resources from domestic and international law enforcement agencies.
- The requested resources will be used primarily to shore up the Special "I" and Technological Crime (TCP) programs. It is anticipated that both Special "I" and TCP will require resources.

B. Technological Crime Program:

- Digital evidence processing as well as the investigations of pure computer crimes are provided through eight (8) Integrated Technological Crime Units (ITCUs) located strategically through out the country and the Technological Crime Branch (TCB) located in Ottawa.
- These specialized teams are seeing unprecedented assistance requests for digital evidence analysis, R&D and custom software tool creation and support. The proposed amendments will exacerbate an already difficult situation. The necessity of increasing the capabilities and capacity of the TCP cannot be over-emphasized.
- TCP will require resources in the Policy and International Coordination area (Ottawa) to address the standards, protocols, policy, liaison and training as well as in the Technical Analysis Team (Ottawa) to provide research, development, verification, validation and/or open and embedded systems analysis.

Annex B

Office of the Director of Public Prosecutions

Funding requirements, specifically in support of the bill, and earmarked in the Fiscal Framework for the ODPP:

Organization Name / Nom de l'organisme : Office of the Director of Public Prosecutions / Bureau du directeur des poursuites pénales							
Input Factor / Facteur d'intrant	**Fiscal Year / Exercice**					**Total**	Ongoing
	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015		
Vote 35 / Crédit 35 (Operating Expenditures / Dépenses de fonctionnement)							
Personnel	2,702,458	2,618,006	2,618,006	2,533,554	2,533,554	**13,005,578**	2,533,554
Operations and Maintenance / Fonctionnement et entretien	832,449	639,831	645,290	629,177	629,177	**3,375,924**	629,177
EBP / RASE (20%)	540,491	523,601	523,601	506,711	506,711	**2,601,115**	506,711
Total -Vote 35 / Total du crédit 35	**4,075,398**	**3,781,438**	**3,786,897**	**3,669,442**	**3,669,442**	**18,982,617**	**3,669,442**
Accommodation / Locaux (13%)	351,320	340,341	340,341	329,362	329,362	**1,690,726**	329,362
Total ODPP	**4,426,718**	**4,121,779**	**4,127,238**	**3,998,804**	**3,998,804**	**20,673,343**	**3,998,804**

The ODPP is requesting $20.67M over five (5) years and $4M ongoing to cover the costs related to the anticipated increase in legal advice requests, increased involvement in the pre-charge stage, an increase in the number of cases referred for prosecution, constitutional challenges, as well as the costs related to the development of new precedents and the training of police officers and prosecutors.

It is anticipated that the use of these new provisions by the police may increase litigation workload in medium and high complexity cases: the defence is expected to challenge the procedure followed by the police in obtaining the new orders with a view to having the evidence excluded.

The ODPP expects that these new provisions may result in more effective investigations and therefore will result in an increase in the number of cases referred to ODPP for prosecution.

Due to the complex and technical nature of these amendments, the ODPP will also dedicate resources to the training of federal prosecutors and the RCMP on the practical impact of the new legislative provisions on investigations and prosecutions. Thus will entail the development of training materials and the use of senior prosecutors and the police. Ongoing and updated delivery of such workshops will be required as the new provisions are adopted into practical use and interpreted by the courts, and as new investigators join units, such as drug squads and Combined Forces Special Enforcement Units (CFSEU), which commonly use these investigative techniques.

ODPP Costing Model

The ODPP estimates that the total impact is 16.8 FTEs of counsel time for the first year (with some reductions with each successive year to 15.7 FTE's in the 4th year and ongoing).

Applying the standard ODPP ratios in costing its litigation workload of the ratio of paralegal and clerical support to Counsel, and iCase data entry support to Counsel and paralegal combined, and in turn, corporate DOJ support, produces a total of 26.2 FTEs when all are included. Note the paralegal and clerical support are directly related to the litigation cases.

Based on the ODPP costing model approved by Treasury Board for use in relation to ODPP cost estimates, these FTEs are then converted to salary and O&M costs, including the ODPP corporate and regional corporate costs. The estimated financial impact on ODPP of amendments of sections 492.1 and 492.2 of the Criminal Code and the creation of new production and preservation orders based on the preceding analysis is estimated to be the following:

2007-2008	2008-2009	2009-2010	2010-2011	2011-2012	5 Year Total
$4,407,324	$4,100,391	$4,106,391	$3,978,629	$3,978,629	$20,571,906

This is based on the costs for the ODPP beginning after the entry into force of the legislation. It should be noted that the cost drops from 2007/08 to 2008/09 since 2007/08 includes the one-time accommodation costs for the new FTEs added in 2007/08, the first full year. In addition, the cost of development of precedents is only a factor for the first full year. The costs associated with constitutional challenges generated by the amendments are reflected in the first three full years, after which the issues should be settled by appellate decisions.

Annex D

Department of Foreign Affairs and International Trade

Organization Name / Nom de l'organisation : Department of Foreign Affairs and International Trade / Ministère des Affairs étrangères et du Commerce international							
Input Factor / Facteur d'intrant	**Fiscal Year / Exercice**					**Total**	Ongoing
	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015		
Vote 1 / Crédit 1 (Operating Expenditures / Dépenses de fonctionnement)							
Personnel	211,200	211,200	211,200	211,200	211,200	**1,056,000**	211,200
Operations and Maintenance / Fonctionnement et entretien	69,104	69,104	69,104	69,104	69,104	**345,520**	69,104
EBP / RASE (20%)	42,240	42,240	42,240	42,240	42,240	**211,200**	42,240
Total -Vote 1 / Total du crédit 1	**322,544**	**322,544**	**322,544**	**322,544**	**322,544**	**1,612,720**	**322,544**
Vote 10 / Crédit 10 (Tranfer Payments / Paiements de transfert)							
Grants / Subventions	0	0	0	0	0	**0**	0
Contributions	300,000	300,000	300,000	300,000	300,000	**1,500,000**	300,000
Total -Vote 10 / Total du crédit 10	**300,000**	**300,000**	**300,000**	**300,000**	**300,000**	**1,500,000**	**300,000**
Accommodation / Locaux (13%)	27,456	27,456	27,456	27,456	27,456	**137,280**	27,456
Total DFAIT	**650,000**	**650,000**	**650,000**	**650,000**	**650,000**	**3,250,000**	**650,000**

Ratification of the Convention and its Additional Protocol

Implementation of the Convention and its Additional Protocol

The International Crime and Terrorism Division (ICT) and the Criminal, Security and Treaty Law Section (JLA) at the DFAIT will be involved in the implementation of the *Convention* and *its Additional Protocol* and other activities related to it. DFAIT is increasingly being called upon to coordinate Canadian policy and positions on cybercrime for international fora, without dedicated personnel to play this role. In particular, DFAIT will be responsible for ensuring that Canadian policy and law are consistent with requirements of the *Convention* and its *Additional Protocol* and Canada's international obligations. DFAIT will also be responsible for providing advice to other departments on the interpretation of the *Convention* and its *Additional Protocol*; and managing the disparate interests of the inter-departmental community to ensure consistent and coordinated foreign policy. DFAIT will respond to requests for assistance and information from other countries; coordinate Canada's reporting obligations to the *Convention* and its *Additional Protocol*; and lead Canadian delegations to the regular Multilateral Consultation meetings among Contracting States to the *Convention* and *its Additional Protocol* to exchange views, review implementation of the *Convention* and *its Additional Protocol* and advise on international legal and policy issues (including on possible amendments to the *Convention* and *its Additional Protocol*). DFAIT will also comment on reports on other States' implementation of the *Convention* and *its Additional Protocol*. ICT expects to be called upon to provide technical assistance and capacity building to other Parties. Most of these activities involve international travel. In addition, DFAIT will be called upon to provide international legal and policy advice in respect of future related international initiatives and international instruments at meetings of a number of international organizations, where the concepts found in the *Convention* and its *Additional Protocol* can migrate into, such as: the UN, the G8, the OAS and the APEC, and also participate in a number of their working groups and committees,

where cybercrime is increasingly discussed. Enhanced anti-cybercrime activity in the hemisphere, for example, will support the advancement of the Americas Strategy.

DFAIT would use the allocated resources to implement the *Convention* and *its Additional Protocol*, to coordinate Canadian positions regarding cybercrime for international fora, and to provide policy advice to technical assistance programmes. Such programming activities will also further Canada's efforts to combat crime, consistent with the objectives of the Americas Strategy. DFAIT will manage the disbursement of funds for cybercrime programming, in collaboration with other government departments, particularly JC, RCMP, and PS, and relevant international partners, under the terms and conditions of the Anti-Crime Capacity Building Program (ACCBP).

International Assistance

An additional $300,000 is being sought for contributions to provide technical assistance to foreign countries to build capacity to combat cyber-crime and/or to facilitate ratification/implementation of the concepts and ideas outlined in the *Convention* and *its Additional Protocol*. Such programming activities will also further the objectives of combating crime within the Americas Strategy. DFAIT will manage the cybercrime programming as a supplement to crime and drug programming currently underway. DFAIT will coordinate the development evaluation of anti-cybercrime programming in cooperation with other government departments (particularly Justice Canada, RCMP, Public Safety Canada) as well as other international partners.

COST MODEL - SUMMARY

Revised: June 2006
(salary table updated 22 Jan 2007)

Organization / Portfolio: Summary
TITLE OF INITIATIVE: Investigative Power of the 21st Century
Activity / Area: *Criminal Code Amendments Initiative*
DATE novembre 8, 2007

Other Staff Base Salary Maximum	Performance Pay 4%	Performance Pay 5%	Increment	Current Year	Current Year + 1	Current Year + 2	Current Year + 3	On-going	2010/11	2011/12	2012/13	2013/14	2014/15
									Salaries as a Function of FTEs				
AS-1 48,430				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
AS-2 51,989				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
AS-3 55,724				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
AS-4 61,047				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
AS-5 72,919				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
AS-6 81,046				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
AS-7 90,420			4,521	0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
AS-8 96,111			4,806	0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
CR-2 34,101				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
CR-3 39,040				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
CR-4 43,286				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
CR-5 47,447				2.0	2.0	2.0	2.0	2.0	94,894	94,894	94,894	94,894	94,894
CS-1 59,817				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
CS-2 72,077				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
CS-3 86,270				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
CS-4 98,803				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
CS-5 118,974				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
ES-1 48,222				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
ES-2 53,207				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
ES-3 64,033				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
ES-4 76,145				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
ES-5 86,681				1.8	1.8	1.8	1.8	1.8	151,692	151,692	151,692	151,692	151,692
ES-6 96,946				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
ES-7 104,938				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
ES-8 112,307				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
IS-1 48,430				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
IS-2 51,989				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
IS-3 61,047				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
IS-4 72,919				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
IS-5 81,046				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
IS-6 90,420				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
SI-1 48,222				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
SI-2 53,207				1.0	1.0	1.0	1.0	1.0	53,207	53,207	53,207	53,207	53,207
SI-3 58,000				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
SI-4 64,033				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
SI-5 76,145				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
SI-6 86,681				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
SI-7 96,946				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
SI-8 104,938				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
Sub-total - Other Staff FTEs				**4.8**	**4.8**	**4.8**	**4.8**	**4.8**	**299,793**	**299,793**	**299,793**	**299,793**	**299,793**
Adjustment for Other Salary Cost Factors													
Bilingual Bonus													
					Derived from supporting sheets				7,920	7,920	7,920	7,920	7,920
Overtime					Derived from supporting sheets				14,990	14,990	14,990	14,990	14,990
Northern Allowance - Salary component					Derived from supporting sheets				-	-	-	-	-
Total - Initiative-specific Salary Costs & FTEs				**13.2**	**13.2**	**13.2**	**13.2**	**13.2**	**1,303,173**	**1,303,173**	**1,303,173**	**1,303,173**	**1,303,173**
NEW "bodies" requiring DOJ workspace (first year only)				7.0	0.0	0.0	0.0	0.0					
2) Initiative-specific O&M Costs													
LA FTE O&M cost factors					Derived from supporting sheets				32,955	32,955	32,955	32,955	32,955
General FTE-related O&M cost factors					Derived from supporting sheets				120,542	120,542	120,542	120,542	120,542
Northern Allowance - O&M component					Derived from supporting sheets				-	-	-	-	-
Training					Derived from supporting sheets				39,095	39,095	39,095	39,095	39,095
Other Exceptional O&M Cost Factors													
Evaluation									22,500	25,000	70,000	27,500	27,500
Audit									-	-	-	-	-
Travel									15,000	16,250	22,500	20,000	20,000
Printing									5,000	5,000	5,000	5,000	5,000
Communications									5,000	5,000	5,000	5,000	5,000
EDP / Furniture									-	-	-	-	-
Consultants									45,000	45,000	25,000	25,000	25,000
Other									86,475	86,248	83,300	81,130	81,130
Total - Initiative-specific O&M Costs									**371,568**	**375,091**	**403,393**	**356,223**	**356,223**
3) Initiative-specific Grants and Contributions (Vote 5)													
Grants									-	-	-	-	-
Contributions									-	-	-	-	-
Total Grants and Contributions									**-**	**-**	**-**	**-**	-

The following sections are formula driven based on information input above.

4) Regional Overhead													
Regional Overhead - Salary													
Derived from supporting sheets				0.0	0.0	0.0	0.0	0.0	-	-	-	-	-
Bilingual Bonus					Derived from supporting sheets				-	-	-	-	-
Total - regional overhead Salary Costs & FTEs				**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**-**	**-**	**-**	**-**	**-**
Regional Overhead - O&M													
General FTE-related O&M cost factors					Derived from supporting sheets				-	-	-	-	-
Training					Derived from supporting sheets				-	-	-	-	-
Accomodation first year fit-up costs					Derived from supporting sheets				-	-	-	-	-
Total - regional overhead O&M									**-**	**-**	**-**	**-**	**-**
5) Corporate Costs													
Corporate o *Salary*					Derived from supporting sheets								
re: provison of services and functional support				1.0	1.0	1.0	1.0	1.0	75,040	75,040	75,040	75,040	75,040
Total Corporate Costs - Salary									**75,040**	**75,040**	**75,040**	**75,040**	**75,040**
Corporate o *O & M*					Derived from supporting sheets				21,841	22,053	23,751	20,920	20,920
Accomodation first year fit-up costs					Derived from supporting sheets				63,734	-	-	-	-
IMB - Help Desk costs					Derived from supporting sheets				19,834	19,834	19,834	19,834	19,834
Total Corporate Costs - O&M									**105,409**	**41,886**	**43,584**	**40,754**	**40,754**
6) TBS - mandated costs													
TBS-mandated Employee Benefit Plan factor					Derived from supporting sheets				275,643	275,643	275,643	275,643	275,643
TBS-mandated PWGSC accomodation costs					Derived from supporting sheets				179,168	179,168	179,168	179,168	179,168
Total TBS-mandated costs									**454,810**	**454,810**	**454,810**	**454,810**	**454,810**

Summary C:\DOCUME~1\000182~1\LOCALS~1\Temp\XPgrpwise\[C-51 Justice summary cost model.xls]Sheet1

				FTE'S					**Dollars**			
FTE's and SALARY												
Initiative Specific				13.2	13.2	13.2	13.2	13.2	1,303,173	1,303,173	1,303,173	1,303,173	1,303,173
Regional Overhead				-	-	-	-	-	-	-	-	-	-
Corporate Costs				1.0	1.0	1.0	1.0	1.0	75,040	75,040	75,040	75,040	75,040
Total FTE and Salary Costs				**14.2**	**14.2**	**14.2**	**14.2**	**14.2**	1,378,213	1,378,213	1,378,213	1,378,213	1,378,213
Employee Benefit Plan			20% of salary costs						275,643	275,643	275,643	275,643	275,643
Total Salary Costs (including EBP)									**1,653,856**	**1,653,856**	**1,653,856**	**1,653,856**	**1,653,856**
O&M													
Initiative Specific									371,568	375,091	403,393	356,223	356,223
Regional overhead									-	-	-	-	-
Corporate costs									105,409	41,886	43,584	40,754	40,754
Total O&M (excluding Accommodation)									**476,977**	**416,977**	**446,977**	**396,977**	**396,977**
								Total salary and O&M (VOTE 1)	**2,130,833**	**2,070,833**	**2,100,833**	**2,050,833**	**2,050,833**
								Total Grants and Contributions (VOTE 5)	**-**	**-**	**-**	**-**	**-**
								TOTAL FOR DEPARTMENT OF JUSTICE	**2,130,833**	**2,070,833**	**2,100,833**	**2,050,833**	**2,050,833**
TBS-mandated PWGSC accomodation costs			13% of salary costs						**179,168**	**179,168**	**179,168**	**179,168**	**179,168**
								TOTAL SUBMISSION (DOJ plus PWGSC)	**2,310,000**	**2,250,000**	**2,280,000**	**2,230,000**	**2,230,000**

INVESTIGATING AND PREVENTING CRIMINAL ELECTRONIC COMMUNICATIONS ACT (PREVIOUSLY BILL C-52)

ISSUE: To provide information on the status of the *Investigating and Preventing Criminal Electronic Communications Act* (Previously Bill C-52).

BACKGROUND:

The Government of Canada's Lawful Access Initiative has two distinct components:

- Public Safety Canada and Industry Canada have primary responsibility for developing new legislation that would compel telecommunication service providers to procure and maintain intercept capable equipment and provide for access to subscriber information;
- Justice Canada has primary responsibility for *Criminal Code* amendments as well as related amendments to other statutes.

Law enforcement agencies face difficulties in consistently accessing subscriber information from telecommunication service providers required to pursue investigations.

Currently, telecommunication service providers (wireline, wireless and internet services) are not required to build interception capability into existing or new networks. Consequently the government must negotiate with and regularly pay telecommunication service providers to create interception solutions for their networks. Additionally, police must often engineer tactical intercept solutions internally before they are able to execute a lawful interception court order. As a result, police are at times unable to execute these court orders.

The proposals contained in the *Investigating and Preventing Criminal Electronic Communications Act* would compel telecommunication service providers to build and maintain intercept capable equipment and provide basic subscriber information to designated police, the Canadian Security Intelligence Service, and Competition Bureau officials upon request.

STRATEGIC CONSIDERATIONS:

The *Investigating and Preventing Criminal Electronic Communications Act* went through first reading in the House of Commons in November, 2010, but subsequently died on the Order Paper. It could be reintroduced in the next session of Parliament. It is expected that warrantless access to subscriber information may be a controversial issue.

INVESTIGATIVE POWERS FOR THE 21ST CENTURY INITIATIVE (PREVIOUSLY BILL C-51)

ISSUE: To provide information on the status of the Investigative Powers for the 21st Century Initiative – Previously Bill C-51 (Lawful Access).

BACKGROUND:

The proposals contained in the Investigative Powers for the 21st Century Initiative (previously Bill C-51) specifically address the ability to investigate and prosecute cybercrime and to collect evidence associated with new technologies.

The Government of Canada's Lawful Access initiative has two distinct components:

- Public Safety Canada and Industry Canada have primary responsibility for developing new legislation that would compel communication service providers to procure and maintain intercept-capable equipment and provide access to subscriber information;
- Justice Canada has primary responsibility for *Criminal Code* amendments as well as related amendments to other statutes.

The use of evolving communications technologies for illicit purposes creates significant public safety challenges. Today's criminal activity often involves the use of mobile phones or computers to send messages through the internet, and digital evidence is often scattered across many devices at various locations. Although there are investigative powers in existing laws that can be utilized, these are out-of-date with the current technology. The Investigative Powers for the 21st Century Initiative will provide better tools for law enforcement, including: preservation demands and orders; transmission data warrants; and new warrants to track transactions, individuals and goods.

The Investigative Powers for the 21st Century Initiative will also allow Canada to ratify the Council of Europe Convention on Cybercrime, an international effort to deal with the global nature of the internet and criminal use of this medium.

CURRENT STATUS:

The Investigative Powers for the 21st Century Initiative was introduced in the House of Commons in November 2010, but subsequently died on the Order Paper. It may be reintroduced in the next session of Parliament.

STRATEGIC CONSIDERATIONS: While the RCMP is not the lead agency, this legislation is critical for combating organized crime. The legislation is aimed at providing police the capability of securing key elements of communications between criminals which has been enhanced through modern technological advancements. It is an important tool for law enforcement, which has lagged behind in its ability to keep pace with technology, and as such should be addressed at the earliest possible opportunity.

NEXT STEPS: The RCMP will continue to work with lead agencies to ensure that they have the necessary information to advance this legislative initiative. Our specific involvement will be based on the requirements identified by the lead agencies.

Royal Canadian Mounted Police  **Gendarmerie royale du Canada**

INVESTIGATIVE POWERS FOR THE 21ST CENTURY INITIATIVE (PREVIOUSLY BILL C-51)

ISSUE:

To provide information on the status of the Investigative Powers for the 21st Century Initiative – previously Bill C-51 (Lawful Access).

BACKGROUND:

The proposals contained in the "Investigative Powers for the 21st Century Initiative" specifically address the ability to investigate and prosecute cybercrime and to collect evidence associated with new technologies.

The Government of Canada's Lawful Access initiative has two distinct components:

- Public Safety Canada and Industry Canada have primary responsibility for developing new legislation that would compel communication service providers to procure and maintain intercept-capable equipment and provide access to subscriber information; and,

- Justice Canada has primary responsibility for *Criminal Code* amendments as well as related amendments to other statutes.

The use of evolving communications technologies for illicit purposes creates significant public safety challenges. Today's criminal activity often involves the use of mobile phones or computers to send messages through the Internet, and digital evidence is often scattered across many devices at various locations. Although there are investigative powers in existing laws that can be utilized, these are out-of-date with the current technology. The Investigative Powers for the 21st Century Initiative will provide better tools for law enforcement, including preservation demands and orders, transmission data warrants, and new warrants to track transactions, individuals and goods.

The Investigative Powers for the 21st Century Initiative will also allow Canada to ratify the Council of Europe Convention on Cybercrime, an international effort to deal with the global nature of the internet and criminal use of this medium.

Updated for Commissioner Paulson
November 2011

CURRENT STATUS:

The Investigative Powers for the 21st Century Initiative was introduced in the House of Commons in November 2010, but subsequently died on the Order Paper. It may be reintroduced in the next parliamentary session.

STRATEGIC CONSIDERATIONS:

While the RCMP is not the lead agency, this legislation is critical for combating organized crime. The legislation is aimed at providing police with the capability of securing key elements of communications between criminals, which has been enhanced through modern technological advancements. This is an important tool for the law enforcement community, which struggles to keep pace with technological advancements.

NEXT STEPS:

The RCMP continues to work with lead agencies to ensure that they have the necessary information to advance this legislative initiative. The RCMP's specific involvement will be based on the requirements identified by the lead agencies.

THE *INVESTIGATING AND PREVENTING CRIMINAL ELECTRONIC COMMUNICATIONS ACT* (PREVIOUSLY BILL C-52)

ISSUE:

To provide information on the status of the *Investigating and Preventing Criminal Electronic Communications Act* (previously Bill C-52).

BACKGROUND:

The Government of Canada's Lawful Access initiative has two distinct components:

- Public Safety Canada and Industry Canada have primary responsibility for developing new legislation that would compel telecommunication service providers to procure and maintain intercept capable equipment and provide for access to subscriber information; and,

- Justice Canada has primary responsibility for *Criminal Code* amendments as well as related amendments to other statutes.

Law enforcement agencies face difficulties in consistently accessing subscriber information from telecommunication service providers required to pursue investigations.

Currently, telecommunication service providers (wireline, wireless and Internet services) are not required to build interception capability into existing or new networks. Consequently, the government must negotiate with, and regularly pay, telecommunication service providers to create interception solutions for their networks.

Additionally, police must often engineer tactical intercept solutions internally before they are able to execute a lawful interception court order. As a result, police are at times unable to execute these court orders.

The proposals contained in the act would compel telecommunication service providers to build and maintain intercept-capable equipment and provide basic subscriber information to designated police, as well as the Canadian Security Intelligence Service and Competition Bureau officials, upon request.

Updated for Commissioner Paulson
November 2011

STRATEGIC CONSIDERATIONS:

The *Investigating and Preventing Criminal Electronic Communications Act* went through first reading in the House of Commons in November 2010, but subsequently died on the Order Paper. It could be reintroduced in the next parliamentary session. It is expected that warrantless access to subscriber information will be a controversial issue.

Royal Canadian Mounted Police / Gendarmerie royale du Canada	File No. / N° de dossier	Security Classification/Designation / Classification/désignation sécuritaire	Total Pages / Pages totales
		Protected A	2

BRIEFING NOTE TO THE COMMISSIONER / **NOTE D'INFORMATION AU COMMISSAIRE**

REINTRODUCE LAWFUL ACCESS LEGISLATION TO REDUCE LAWFUL ACCESS AND ELECTRONIC SURVEILLANCE DEFICIENCIES AND OBSOLESCENCE

ISSUE: To brief the Commissioner on the Canadian Association of Chiefs of Police (CACP) Resolution in support of the Investigative Powers for the 21st Century (IP21C) legislation (formerly Bill C-51) for the CACP Conference in August 2011.

BACKGROUND:

- Current *Criminal Code* provisions in respect to police powers to conduct judicially authorized electronic interceptions and seizures are outdated, especially with the advent of new and evolving technologies.
- The proposals contained in IP21C specifically address the ability to investigate and prosecute cybercrime and to collect evidence associated with new technologies.
- The legislation impacts two specific programs within the RCMP, Special "I" and the Technological Crime Program.
- IP21C will also allow Canada to ratify the Council of Europe Convention on Cybercrime, an international effort to deal with the global nature of the Internet and the criminal use of this medium.

CURRENT STATUS:

- IP21C went through a first reading in the House of Commons in November 2010, but died on the Order Paper when Parliament was dissolved in March 2011. It could be reintroduced at any time during the next session of Parliament.

STRATEGIC CONSIDERATIONS:

- Without modernization, the current legislation challenges police investigative techniques and compromises public safety. Urgent amendments are required to allow the police to lawfully and effectively investigate serious offences; particularly those committed by organized crime and terrorist groups. This applies to interception capabilities as well as the ability to investigate cybercrime incidents which are both addressed in this proposed legislation.
- The RCMP has worked diligently over many years with Public Safety Canada in an attempt to fill this legislative void.

Submitted by – Rédigé par	Date	Recommended by – Recommandé par	Date
Stan Burke, C/Supt. DG Technical Investigations Services	2011-08-04	Antoine Babinsky, A/Commr. Technical Operations	2011-08-04
Approved by – Approuvé par Line Carbonneau, D/Commissioner Policing Support Services	Date 2011.08.05		

File No. N° de dossier	Security Classification/Designation Classification/désignation sécuritaire Protected A

RECOMMENDATIONS/STRATEGIC ADVICE:

- The RCMP should support the CACP Resolution to endorse the passage of this legislation.

BN Identification # TechOps 11-041 CCM# 11- 003054

Royal Canadian Mounted Police / Gendarmerie royale du Canada	File No. / N° de dossier	Security Classification/Designation / Classification/désignation sécuritaire	Total Pages / Pages totales
		Protected A	2

BRIEFING NOTE TO THE COMMISSIONER — **NOTE D'INFORMATION AU COMMISSAIRE**

INTRODUCE ELECTRONIC COUNTERMEASURES LEGISLATION

ISSUE: To provide the Commissioner with an update for the Canadian Association of Chiefs of Police (CACP) Conference in August 2011 on the Radio Frequency Electronic Counter Measures program as it relates to the CACP Resolution to introduce electronic countermeasures legislation

BACKGROUND:

- The *Radiocommunication Act* prohibits the possession, installation or operation of jamming/interference technological apparatus as well as the interference or obstruction of any radiocommunication.
-
-

CURRENT STATUS:

- CBRNE Operations is actively working with Industry Canada, Public Safety Canada, and "A" Division Federal Enforcement Section (FES) to formulate an efficient prosecution policy.

Submitted by - Rédigé par	Date	Recommended by - Recommandé par	Date
Kenneth Faulkner, A.OIC CBRNE Operations	2011-08-03	Antoine Babinsky, A/Commr. Technical Operations	2011-08-03
Approved by - Approuvé par Line Carbonneau, D/Commr, Policing Support Services	Date 2011-08-05		Date

CONSULT

A0271017_60-000065

File No. N° de dossier	Security Classification/Designation Classification/désignation sécuritaire Protected A

-

- CBRNE Operations recommends that TCRI policies be reviewed and upgraded to properly formulate the investigational procedures required for successful prosecutions. CBRNE Operations will update the existing operational policy, and will assist FES in updating the RCMP's related investigative policies.

- Canada Border Services Agency (CBSA) is interested in assisting and participating actively to resolve the influx of illegal jammers entering Canada via the points of entry.

- Industry Canada has identified an urgent need to enhance enforcement capabilities and is seeking the creation of an integrated investigative unit. The RCMP has taken a leadership role to develop a joint-partnership initiative and supports the creation of an integrated unit between its CBRNE Operations, Federal Enforcement Sections (FES) and the CBSA.

STRATEGIC CONSIDERATIONS:

-

- The possession and use of commercially purchased RF jamming units by the criminal element and the general public place police personnel and the community at risk. Unauthorized RF interference impacts on the ability of the RCMP and provincial/municipal police agencies to perform their lawful duties.

RECOMMENDATIONS/STRATEGIC ADVICE:

- The RCMP supports and encourages the CACP to adopt the resolution to introduce electronic countermeasures legislation.

BN Identification # TechOps 11-038 CCM# 11- 003054

Royal Canadian Mounted Police / Gendarmerie royale du Canada

File No. / N° de dossier	Security Classification/Designation / Classification/désignation sécuritaire	Total Pages / Pages totales
	Protected "A"	1

BRIEFING NOTE TO THE COMMISSIONER / **NOTE D'INFORMATION AU COMMISSAIRE**

CANADIAN TRAINING STANDARDS FOR CHILD EXPLOITATION INVESTIGATORS

ISSUE: To brief the Commissioner on the Canadian Association of Chiefs of Police (CACP) E-Crime Committee's Resolution on Canadian training standards for child exploitation investigators for the CACP Conference in August 2011.

BACKGROUND:

- Although standardized training programs exist, disparities exist amongst Canadian law enforcement agencies in the application and enforcement of standardized training for child exploitation investigators.

CURRENT STATUS:

- The Canadian Police College (CPC) provides training courses which are necessary to enable all police organizations to provide child exploitation investigation services. These courses must be properly funded and equipped to provide this specialized training in both official languages as required.

STRATEGIC CONSIDERATIONS:

- The investigation of child exploitation cases by untrained, partially trained or self-trained investigators who do not follow training standards and methodologies can potentially be a significant risk for the Canadian law enforcement community. Issues could include a loss of public confidence in the investigative capability of police agencies and questions surrounding procedural fairness, possibly bringing the administration of justice into disrepute.
- Child exploitation crimes have become an issue of national and international significance, demanding the attention of law enforcement agencies and the criminal justice system.

STRATEGIC ADVICE:

- The RCMP should support the E-Crime Committee's resolution to ensure a safe and secure Internet for Canadians.
- Law enforcement agencies initiating child exploitation investigations should be encouraged to undertake these functions only with personnel who have met the recommended training standards of the CPC Technological Crime Learning Institute Program or other validated training.

BN Identification #: TechOps 11-039 CCM# 11- 003054

Submitted by – Rédigé par	Date	Recommended by – Recommandé par	Date
C/Supt. Stan Burke D.G. Technical Investigative Services	2011-08-03	Antoine Babinsky, A/Commr. Technical Operations	2011-08-03
Approved by – Approuvé par Line Carbonneau, D/Commr. Policing Support Services	Date 2011.08.05		

CONSULT

Speaking Notes
for the

Honourable Peter Van Loan
Minister of Public Safety

For an appearance before the Standing Committee on Public Safety and National Security (SECU)

Review of Bill C-47

An Act regulating telecommunications facilities to support investigations
(Technical Assistance for Law Enforcement in the 21st Century Act)

Ottawa, ON

November 19, 2009

Check against delivery

Thank you, Mr. Chairman, for the invitation to appear before this committee. It's always a pleasure to be here. I'm especially happy that you have asked me here today to assist with your review of Bill C-47, *an Act Regulating Telecommunication Facilities to Support Investigations.* With me are senior officials from the Portfolio. [*Introduce officials.*]

Bill C-47, of course, is designed primarily to do one thing – help victims of crime. That includes many children who today remain vulnerable to exploitation by sexual predators online because the laws now in place don't give law enforcement officials the tools they need to do their jobs. Hon. Committee members

may have heard of the case where Germany alerted Canadian law-enforcement officials that 200 IP addresses were associated with online child exploitation as part of a massive world-wide investigation of child pornography. The RCMP requested information from Internet service providers to help them identify potential suspects. Unfortunately, 47 of those requests were refused since it was deemed that there was insufficient information to obtain warrants

and today countless children remain at risk.

Some Hon. Committee members might also know about another international criminal investigation involving 78 Canadian IP addresses linked to the purchase of child pornography. In that case, requests for customer name and address information were submitted to the relevant Internet Service Providers and there were several arrests and charges. But again, 18 of the original 44 suspects have not been identified since ISPs refused to provide the relevant information without a warrant – something normally granted only **after** the identify of a suspect is established.

Such cases clearly demonstrate the need for reforms. They show the need to bring our laws up to date with the realities of the 21st century. That's what Bill C-47 will do. The legislation before us today will first and foremost help victims by ensuring criminals such as sexual predators can't remain anonymous and escape prosecution. Today, some ISPs comply with requests for customer information without a warrant. Many don't. What Bill C-47 therefore proposes is to establish a uniform requirement for all ISPs to provide law enforcement officials with quick and timely access to subscriber information without the need for a warrant. The courts have come down in favour of allowing this.

Stakeholders, victim's advocacy groups and police associations have asked for and support these changes – as do many ordinary Canadians. Bill C-47 delivers on our commitment to them, while also ensuring privacy rights are protected through a series of rigorous safeguards which reinforce the considerable legal protection currently afforded to Canadians with respect to privacy or freedom from unreasonable search and seizure.

Bill C-47, of course, also proposes to help victims by doing away with so-called "safe havens" which currently allow sexual predators, perpetrators of hate crime, organized crime groups, and Internet fraud

artists to operate freely without any fear of detection and apprehension. Specifically, the Bill before us today will ensure that when law enforcement and security officials have a warrant to intercept messages by criminals or terrorists, they are not prevented from doing so due to a lack of technical ability.

The previous government introduced similar provisions, recognizing the need to give public safety officials the tools they require to do their jobs. While it was a good start, Bill C-47 builds on that effort and strengthens it further.

The proposals we are putting forward are not new or even revolutionary. In modernizing Canada's lawful access laws, we are not providing new powers or expanding on existing interception authorities that have been in place since 1974. Nor are we compromising individuals' personal information or putting an undue burden on business. We are simply bringing our country's legislation out of the Cold War era and into the 21st Century.

Together with the changes proposed in Bill C-46, which this committee will soon have a chance to review, the message that we are sending with these proposed changes is that helping victims is our

number one priority. We're saying that the rights of victims should come ahead of those of criminals who are currently able to exploit technologies to their advantage. Standing up for the victims of crime has always been at the heart of this government's public safety and justice agenda. Our government is committed to ensuring that their voices are heard and that their concerns are taken seriously. That is one of our highest priorities and why we've taken action on a number of fronts. Bill C-47 builds on and strengthens this track record and I know in this regard has the support of all Hon. Committee Members as well as Canadians right across this country. I therefore look forward to working with this

committee over the coming weeks to ensure speedy passage of this vitally important legislation.

Thank you.

From: "Sellers, Philip" <Philip.Sellers@ps-sp.gc.ca>
To: "'Susan.Alter@rcmp-grc.gc.ca'" <Susan.Alter@rcmp-grc.gc.ca>, "'Brigitte.Mineault@rcmp-grc.gc.ca'" <Brigitte.Mineault@rcmp-grc.gc.ca>, "'Roberta.Sinclair@rcmp-grc.gc.ca'" <Roberta.Sinclair@rcmp-grc.gc.ca>
CC: "Goguen, Taunya" <Taunya.Goguen@ps-sp.gc.ca>, "'Bernard.Tremblay@rcmp-grc.gc.ca'" <Bernard.Tremblay@rcmp-grc.gc.ca>, "Desnoyers, Christine" <christine.desnoyers@rcmp-grc.gc.ca>, "'Debra.Robinson@rcmp-grc.gc.ca'" <Debra.Robinson@rcmp-grc.gc.ca>, "'Elisa.Bernstein@rcmp-grc.gc.ca'" <Elisa.Bernstein@rcmp-grc.gc.ca>, "Spendlove, Jim" <Jim.Spendlove@rcmp-grc.gc.ca>, "'john.bilinski@rcmp-grc.gc.ca'" <john.bilinski@rcmp-grc.gc.ca>, "'Luc.Vidal@rcmp-grc.gc.ca'" <Luc.Vidal@rcmp-grc.gc.ca>, "'Mike.Gaudreau@rcmp-grc.gc.ca'" <Mike.Gaudreau@rcmp-grc.gc.ca>, "'Ray.Bonnell@rcmp-grc.gc.ca'" <Ray.Bonnell@rcmp-grc.gc.ca>, "'Tom.Pownall@rcmp-grc.gc.ca'" <Tom.Pownall@rcmp-grc.gc.ca>
Date: 11/16/2009 6:33 PM
Subject: Re: RE: Minister of PS Speaking Notes

Ps
Many thanks again for all the input
As explained to Roberta, the MO in this case has some very definite ideas on the messaging and examples they want to use and again after my chat with Roberta she can probably provide you with morr info than I can from an email
Again if you want to talk with me directly don't hesitate to call me Tuesday
Many thanks again!!

----- Original Message -----
From: Sellers, Philip
To: 'Susan.Alter@rcmp-grc.gc.ca' <Susan.Alter@rcmp-grc.gc.ca>; 'Brigitte.Mineault@rcmp-grc.gc.ca' <Brigitte.Mineault@rcmp-grc.gc.ca>; 'Roberta.Sinclair@rcmp-grc.gc.ca' <Roberta.Sinclair@rcmp-grc.gc.ca>
Cc: Goguen, Taunya; 'Bernard.Tremblay@rcmp-grc.gc.ca' <Bernard.Tremblay@rcmp-grc.gc.ca>; 'christine.desnoyers@rcmp-grc.gc.ca' <christine.desnoyers@rcmp-grc.gc.ca>; 'Debra.Robinson@rcmp-grc.gc.ca' <Debra.Robinson@rcmp-grc.gc.ca>; 'Elisa.Bernstein@rcmp-grc.gc.ca' <Elisa.Bernstein@rcmp-grc.gc.ca>; 'Jim.Spendlove@rcmp-grc.gc.ca' <Jim.Spendlove@rcmp-grc.gc.ca>; 'john.bilinski@rcmp-grc.gc.ca' <john.bilinski@rcmp-grc.gc.ca>; 'Luc.Vidal@rcmp-grc.gc.ca' <Luc.Vidal@rcmp-grc.gc.ca>; 'Mike.Gaudreau@rcmp-grc.gc.ca' <Mike.Gaudreau@rcmp-grc.gc.ca>; 'Ray.Bonnell@rcmp-grc.gc.ca' <Ray.Bonnell@rcmp-grc.gc.ca>; 'Tom.Pownall@rcmp-grc.gc.ca' <Tom.Pownall@rcmp-grc.gc.ca>
Sent: Mon Nov 16 18:19:27 2009
Subject: Re: RE: Minister of PS Speaking Notes

Ms. Alter
I have spoken with Roberta
Please touch base with her with regard to the speech.
Many thanks.

----- Original Message -----
From: Susan Alter <Susan.Alter@rcmp-grc.gc.ca>
To: Sellers, Philip; Brigitte Mineault <Brigitte.Mineault@rcmp-grc.gc.ca>; Roberta Sinclair <Roberta.Sinclair@rcmp-grc.gc.ca>
Cc: Goguen, Taunya; Bernard Tremblay <Bernard.Tremblay@rcmp-grc.gc.ca>; Desnoyers, Christine; Debra Robinson <Debra.Robinson@rcmp-grc.gc.ca>; Elisa Bernstein <Elisa.Bernstein@rcmp-grc.gc.ca>; Spendlove, Jim; John Bilinski <john.bilinski@rcmp-grc.gc.ca>; Luc Vidal <Luc.Vidal@rcmp-grc.gc.ca>; Mike Gaudreau <Mike.Gaudreau@rcmp-grc.gc.ca>; Ray Bonnell <Ray.Bonnell@rcmp-grc.gc.ca>; Tom Pownall <Tom.Pownall@rcmp-grc.gc.ca>
Sent: Mon Nov 16 16:59:18 2009
Subject: RE: RE: Minister of PS Speaking Notes

Mr. Sellers,

Best regards,

Susan

Susan Alter, Senior Counsel /
Avocate-conseil
RCMP Legal Services /
Services juridiques GRC
Department of Justice /
Ministère de la Justice
Ottawa, Canada K1A 0R2
susan.alter@rcmp-grc.gc.ca
Telephone /Téléphone 613-990-9090
Facsimile /Télécopieur 613-990-2343
Government of Canada / Gouvernement du Canada

>>> "Sellers, Philip" <Philip.Sellers@ps-sp.gc.ca> 11/16/2009 2:39 PM
>>>
Sorry. Not sure what all this refers to. The one example which RCMP highlighted needed amending has been changed as per the attached and according to your suggested wording. Public Safety has the lead on this file and this has now been signed off at the ADM level. We had forwarded this to Jim to ask that the examples only be looked at and as mentioned changes have been incorporated according to your suggestions.

Philip Sellers
Senior Speech Writer - Rédacteur de discours principal
Public Safety Canada - Sécurité Publique Canada
11C-3400
269 Laurier Ave. West
Ottawa, ON.
Phone: 613-949-1672
Philip.sellers@ps-sp.gc.ca

-----Original Message-----
From: Roberta Sinclair [mailto:Roberta.Sinclair@rcmp-grc.gc.ca]
Sent: November 16, 2009 2:26 PM
To: Brigitte Mineault
Cc: Sellers, Philip; Goguen, Taunya; Bernard Tremblay; Desnoyers, Christine; Spendlove, Jim; John Bilinski; Luc Vidal; Ray Bonnell; Susan Alter; Tom Pownall
Subject: Fwd: RE: Minister of PS Speaking Notes

Hello Brigitte,

Upon reviewing the revised speech from PS, the CPCMEC management team must again raise our concerns over the content of said document.

Tech Ops is the Lead policy centre for Bill C-47 and should be consulted as to the accuracy of the statements within the Bill.

The CPCMEC can only comment on the child sexual exploitation components. I have attached a copy of the CNA examples that had been prepared - this document should be consulted by the speech writer to ensure accuracy of statement in terms of examples. If further clarification regarding the approved examples is required we can provide
that. As well, the RCMP dec provided in July should provide guidance as
to key messages (see attached).

The concerns we expressed last week still remain and we would caution against this version going forward. Due to time constraints provided there is not sufficient time to provide detailed comments.

Roberta

>> Brigitte Mineault 11/16/2009 11:01 AM >>>
Hi everyone,

Here is the revised speech from PS. There's a tight turnaround time on
this so if you could have a look and send it back as soon as you can, that would be great.

Merci

Brigitte Mineault
Communications Team Lead, Policing Support Services/Chef d'équipe en Communications, Soutien aux Services de Police

National Communications Services /Services Nationaux de Communication
RCMP/GRC
Tel: 613-949-0285
Cell: 613-298-9264

Roberta Lynn Sinclair, Ph.D.
Canadian Police Centre for Missing and Exploited Children
Manager, Research and Development Unit
890 Taylor Creek Road, A-9
Orleans, Ontario
K1A 0R2

Phone: (613) 841-1342
Fax: (613) 841-0553

>>> "Sellers, Philip" <Philip.Sellers@ps-sp.gc.ca> 11/16/2009 10:55 AM >>>

Jim, this is OK but will need this back by no later than 2:00 today since it also has to go to DM and Associate.

Philip Sellers
Senior Speech Writer - Rédacteur de discours principal
Public Safety Canada - Sécurité Publique Canada
11C-3400
269 Laurier Ave. West
Ottawa, ON.
Phone: 613-949-1672
Philip.sellers@ps-sp.gc.ca

-----Original Message-----
From: Spendlove, Jim
Sent: November 16, 2009 10:05 AM
To: Sellers, Philip
Cc: Brigitte Mineault; Luc Vidal; Roberta Sinclair
Subject: RE: Minister of PS Speaking Notes

Hi Phil: Given that the speech goes into some detail about NCECC, they've asked to review the final draft . Trsut this is OK with you
Thanks

Jim

>>> "Sellers, Philip" <Philip.Sellers@ps-sp.gc.ca> 11/13/2009 9:54 AM >>>
Hi Jim, sorry not to get back to you yesterday
I think we should be OK in terms of reviewing the content since your folks have reviewed the examples, we have had the content reviewed by legal, and both the DM and Associate will also review. Will send final once it is ready to go.

Cheers and many thanks for the help!!

Philip Sellers
Senior Speech Writer - Rédacteur de discours principal
Public Safety Canada - Sécurité Publique Canada
11C-3400
269 Laurier Ave. West
Ottawa, ON.
Phone: 613-949-1672
Philip.sellers@ps-sp.gc.ca

-----Original Message-----
From: Spendlove, Jim
Sent: November 12, 2009 2:21 PM
To: Sellers, Philip
Cc: Bernard Tremblay; Brigitte Mineault; Roberta Sinclair; Sean Pope; Susan Alter; Tim Cogan
Subject: RE: Minister of PS Speaking Notes

Hi Phil: NCECC had no additional comments...would you like the speaking
points reviewed again once they're revised? Thx

Jim

>>> "Sellers, Philip" <Philip.Sellers@ps-sp.gc.ca> 11/12/2009 12:45 PM
>>>
Many thanks!!

Philip Sellers
Senior Speech Writer - Rédacteur de discours principal
Public Safety Canada - Sécurité Publique Canada
11C-3400
269 Laurier Ave. West
Ottawa, ON.
Phone: 613-949-1672
Philip.sellers@ps-sp.gc.ca

-----Original Message-----
From: Spendlove, Jim
Sent: November 12, 2009 12:43 PM
To: Sellers, Philip
Cc: Bernard Tremblay; Brigitte Mineault; Sean Pope; Susan Alter; Tim Cogan
Subject: Fwd: Minister of PS Speaking Notes

Phil: Please see attached comments, speaking notes (changes highlighted), and Deck...we are waiting to see if there are any further
suggestions from NCECC. Thanks!
Jim

From: Jennifer TURNER
To: KONOWALCHUK, Dan
Date: 7/28/2009 2:54 PM
Subject: Fwd: Lawful Access
Attachments: Lawful Access

Good afternoon, Dan. An example, circumstances as follows:

Hope this helps.

Jennifer

Sgt. Jennifer J. Turner
Operational Support NCO
Leduc Detachment
#1-4119-50 Street, Leduc, AB.T9E 7L9
WK: 780-980-7203
CELL: 780-292-5824

>>> Thomas WITZKE (Annette) (Thomas WITZKE) 2009-07-28 12:13 >>>
Operational Members Only

Annette
for,

S/Sgt. Tom WITZKE
Operations NCO
Leduc Detachment
Phone: 780-980-7207
Cell: 780-916-2815
Fax: 780-986-9569
Email: thomas.g.witzke@rcmp-grc.gc.ca

>>> B.K. MCLEOD 2009-07-28 08:33 >>>
Commanders,
please share with your personnel whom have had experience with technical investigative need. Present day legislation is totally out dated and law enforcement agencies urgently need a modernization of electronic/technical investigative techniques to effectively address today's crime trends. Should any of your personnel have investigations as examples in support of legislation, please forward directly to Insp. Konwalchuk....thank you,bkmc.

>>> Wade BLAKE 2009-07-22 14:16 >>>
FYI & any response to Kono!
Tks!

>>> Dan KONOWALCHUK 2009-07-22 13:02 >>>
Ladies and Gentlemen.

The attached is self-explanatory. We are looking for any stories/examples which would further support the proposed legislation.

Please pass this along to all of your operational units. I would invited people to respond to me directly and I will coordinate a response to S/Sgt. Nyenhuis.

Thanks,

Dan Kono

>>> Joseph LORAN 2009-07-22 10:25 >>>
Dan,

The attached would refer mainly to your area and the support you provide to other units. Please review and if appropriate provide a response with a cc to the I & I Officer. This may require some consultation with the investigative units to whom the assistance was provided.

Thank you,

Joe Loran

>>> Bill SMITH 2009-07-22 06:45 >>>
We should help if and where we can.

Bill

From: Craig A. MCINTYRE
To: BOYLE, Nancy; DELORENZO, Dina; LESTER, Deryn; VAN DUSEN, Edna
Date: 7/23/2009 9:42 AM
Subject: Fwd: Lawful Access
Attachments: Fwd: Lawful Access

CC: KONOWALCHUK, Dan

Good morning,

This request would pertain more to yourselves as you are more directly involved in requesting Customer Name & Address Information (CNA).

I don't entirely agree with one portion of the message which states:
" Although the present state of the law is that such information does not require a warrant and can be provided to police voluntarily, the experience by your investigators is that compliance with requests is inconsistent and at times obstructionist. "

There is no distinction in this message between Published & Non-Published numbers which do require warrant.

Other than that minor point, as requested, if any of you have had experience in dealing with a Telco & are able to provide:

"actual examples where access to CNA has either provided an effective and important aspect to an investigation or, in the alternative, where refusal by a company to provide the information has hindered an investigation or threatened public safety.", please forward them to myself & I will ensure they are sent through to Insp Konowalchuk.

Thanks.

Craig

From: Jeff CAMERON
To: KONOWALCHUK, Dan
Date: 5/21/2009 1:50 PM
Subject: Fwd: Re: IP Trace

Please add to my file....

I should also brief you on this file as I think it will be the subject of a Briefing Note to Crops from members.

Jef

Cpl. Jeff Cameron
Calgary Technological Crime Unit
7575 8th Street N.E.
Calgary, Alberta
T2E 8A2
Desk (403)230-6435
Cell (403)470-9730
E Mail jeffc@abtechcrime.comf
>>> Richard Leclair 2009-05-19 12:49 >>>
Jeff,

Many Thanks for the excellent work.

We'll let our LLB membership discuss matter with their NCO I/C, maybe Crown, and see how they see matter unfold.

Kind Regards,

Cpl. Richard LECLAIR
Interpol Ottawa
Crime Section
613-949-4610

>>> Jeff CAMERON 2009-05-19 2:40 PM >>>

If you have any questions feel free to contact me directly at (403)230-6435.

Thx
Jeff

Cpl. Jeff Cameron
Calgary Technological Crime Unit
7575 8th Street N.E.
Calgary, Alberta
T2E 8A2
Desk (403)230-6435
Cell (403)470-9730
E Mail jeffc@abtechcrime.com

From: Elisa Bernstein
To: O'Reilly, Rob
Date: 7/24/2009 4:10 PM
Subject: Re: Fwd: Lawful Access / CACP

CC: Flynn, Mark; Gaudreau, Mike; Giguere, Pierre; Konarski, Tom; Routhier, Carole; Tremblay, Bernard

Hi again Rob,

Also we are coordinating a new repository of examples between our organizations.

I hope this is sufficient and we can avoid tasking the field sections in this instance.

Elisa

>>> Rob O'Reilly 7/24/2009 2:17 PM >>>
Thanks Elisa.

>>> Elisa Bernstein July 24, 2009 2:16 PM >>>

This may be a short time line, but I know they have gone across the country very recently, in preparation with our meeting with the assistance Privacy Commissioner and have many developed examples that can assist.

I'll contact the Calgary officer myself, he knows Tom and Mark well. I'll ensure that it's communicated that the RCMP will provide any examples required, in two weeks. I wouldn't advise taking the Divisions as we have the information.

Elisa

>>> Bruce Rogerson 7/24/2009 1:53 PM >>>
Mike,

I was just speaking with Rob O'Reilly, EA to D/Commr. Killam. What he wants is for us to contact Calgary Police Services (writer on the attached) and find out the scope of their requests and get than to get back to him with the requirements. EBS will then task the appropriate policy centre.

Thank you.
Carole.

>>> Rob O'Reilly 7/23/2009 3:04 PM >>>
Sir,

This message came in from the CACP yesterday and was discussed amongst the deputies last night. Due to our prior extensive involvement on this (Commissioner, Minister, Privacy Commissioner) PSS has been appointed to coordinate the response for the RCMP. EBS will coordinate the tasking, however the Deputy would like to reach out to the CACP committee member named within to ascertain the scope of our response. For example, should we be tasking this out to CROPS Officers across the country, and if so what type of examples should we ask them to focus on?

Thanks,

Rob

From: Dan KONOWALCHUK
To: Flynn, Mark; Konarski, Tom
Date: 8/25/2009 2:38 PM
Subject: Lawful Access
Attachments: Fwd: Lawful Access; Re: Fwd: Lawful Access; Fwd: Lawful Access ; Fwd: Lawful Access; Lawful Access DD: TODAY; Re: Fwd: Lawful Access; Fwd: Lawful Access; Fwd: Re: IP Trace 2009500782

CC: Bernstein, Elisa; LORAN, Joseph

Good morning gents.

The attached messages are some examples/comments which may be of assistance. Some issues raised are already well known and some are not completely topical, however I have included them in order to be inclusive or in some case re-emphasize same should you feel appropriate to include.

I have not included the many nil responses received.

Regards,

Dan Konowalchuk
Covert Operations
"K" Division

Bonjour , J'aimerais remercier Ministre Van Loan et Mme Brisebois de m'avoir invité aujourd'hui pour vous parler sur le sujet de la la securité et les crimes sur l'Internet. Les commentaires de notre Ministre sont très a propos.

My name is Tom Pownall and I'm the Officer in Charge of the RCMP Technological Crime Branch, which manages the RCMP Tech Crime Program and leads the RCMP Cyber Crime Council.

Our Cyber Crime Council brings together all RCMP investigative Programs that are responsible to deal with cyber crime.

Cyber Crime includes all crimes that can be committed or facilitated with Internet based technologies. Just as we use the Internet for legitimate communications and personal and business activities, criminals are using the Internet for illegal purposes.

In today's world virtually all crimes can be facilitated with the Internet. Criminals can use the internet to communicate, plan activities, recruit conspirators, raise/move/or launder funds and commit criminal acts.

This includes national security criminal acts, organized crimes including financial crimes such as fraud and identity theft and child exploitation.

Since the Internet and technology can facilitate all types of crime, no single investigative police unit can be responsible for the prevention, detection and investigation. Within the RCMP operational model, the investigative program responsible for the substantive criminal act leads the investigative response and they are supported by forensic experts from the technological crime program.

For example, investigations into on-line fraud are led by fraud investigators and computer forensic experts from the Tech Crime Program support them with the technical expertise that they require to search, seize and analyse the digital evidence and Internet based evidence.

In the same manner child exploitation investigations are led by specialists in the investigation of child exploitation and computer forensic experts from the Tech Crime Program support them with the technical expertise that they require to search, seize and analyse the digital evidence and Internet based evidence.

This model ensures that all investigations are led by experts in their specific crime type and supported by subject matter experts in technology.

We have specialized investigators and forensic experts located across the country to conduct cyber crime investigations.

Of course cyber crime is a global phenomenon, and we also work closely with our international partners through Interpol, and in specific work groups such as the G8 and the Strategic Alliance Cyber Crime Work Group which brings together our partners in the US, UK, Australia and New Zealand.

The elements of our cyber crime enforcement program include:

- Crime prevention and awareness
- Specialized Training
- Best practices in intelligence and investigations
- And criminal prosecution

The focus on crime prevention is why cyber security awareness month is such an excellent initiative of Public Safety Canada.

The first and foremost element of our cyber crime program is – Crime prevention and awareness. If we can be proactive and work together with the citizens, businesses, Internet service providers and our other partners to prevent cyber crime, then we've really done our job in protecting Canadians on-line.

In terms of cyber crime prevention, my advice is to ensure that the public and businesses ensure that they keep their operating systems up to date with the latest updates to fix vulnerabilities, and to ensure that they have current firewalls, anti-virus software, malware protection and spyware protection. Additional information on this is available at publicsafety.ca or on the RCMP web page.

And finally, if you believe that you may be a victim of a cyber crime, please contact your local police service.

Merci/Thank you

xxxx

C-52

Third Session, Fortieth Parliament,
59 Elizabeth II, 2010

HOUSE OF COMMONS OF CANADA

BILL C-52

An Act regulating telecommunications facilities to support investigations

FIRST READING, NOVEMBER 1, 2010

MINISTER OF PUBLIC SAFETY

90523

C-52

Troisième session, quarantième législature,
59 Elizabeth II, 2010

CHAMBRE DES COMMUNES DU CANADA

PROJET DE LOI C-52

Loi régissant les installations de télécommunication aux fins de soutien aux enquêtes

PREMIÈRE LECTURE LE 1ER NOVEMBRE 2010

MINISTRE DE LA SÉCURITÉ PUBLIQUE

RECOMMENDATION

His Excellency the Governor General recommends to the House of Commons the appropriation of public revenue under the circumstances, in the manner and for the purposes set out in a measure entitled "*An Act regulating telecommunications facilities to support investigations*".

RECOMMANDATION

Son Excellence le gouverneur général recommande à la Chambre des communes l'affectation de deniers publics dans les circonstances, de la manière et aux fins prévues dans une mesure intitulée « *Loi régissant les installations de télécommunication aux fins de soutien aux enquêtes* ».

SUMMARY

This enactment requires telecommunications service providers to put in place and maintain certain capabilities that facilitate the lawful interception of information transmitted by telecommunications and to provide basic information about their subscribers to the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, the Commissioner of Competition and any police service constituted under the laws of a province.

SOMMAIRE

Le texte exige des télécommunicateurs qu'ils disposent des moyens nécessaires pour faciliter l'interception licite de l'information transmise par télécommunication et qu'ils fournissent des renseignements de base sur leurs abonnés à la Gendarmerie royale du Canada, au Service canadien du renseignement de sécurité, au commissaire de la concurrence ou à tout service de police constitué sous le régime d'une loi provinciale.

Also available on the Parliament of Canada Web Site at the following address:
http://www.parl.gc.ca

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :
http://www.parl.gc.ca

TABLE OF PROVISIONS

AN ACT REGULATING TELECOMMUNICATIONS FACILITIES TO SUPPORT INVESTIGATIONS

TABLE ANALYTIQUE

LOI RÉGISSANT LES INSTALLATIONS DE TÉLÉCOMMUNICATION AUX FINS DE SOUTIEN AUX ENQUÊTES

3rd Session, 40th Parliament,
59 Elizabeth II, 2010

HOUSE OF COMMONS OF CANADA

BILL C-52

An Act regulating telecommunications facilities to support investigations

Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows:

SHORT TITLE

Short title

1. This Act may be cited as the *Investigating and Preventing Criminal Electronic Communications Act*.

INTERPRETATION

Definitions

2. (1) The following definitions apply in this Act.

"authorized" *« autorisée »*

"authorized", in relation to a person, means having authority, under the *Criminal Code* or the *Canadian Security Intelligence Service Act*, to intercept communications.

"communication" *« communication »*

"communication" means a communication effected by a means of telecommunication and includes any related telecommunications data or other ancillary information.

"intercept" *« intercepter »*

"intercept" includes listen to, record or acquire a communication or acquire the substance, meaning or purport of the communication.

"Minister" *« ministre »*

"Minister" means the Minister of Public Safety and Emergency Preparedness.

"person" *« personne »*

"person" includes a partnership, an unincorporated organization, a government, a government agency and any other person or entity that acts in the name of or for the benefit of another.

90523

3e session, 40e législature,
59 Elizabeth II, 2010

CHAMBRE DES COMMUNES DU CANADA

PROJET DE LOI C-52

Loi régissant les installations de télécommunication aux fins de soutien aux enquêtes

Sa Majesté, sur l'avis et avec le consentement du Sénat et de la Chambre des communes du Canada, édicte :

TITRE ABRÉGÉ

Titre abrégé

1. *Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention.*

DÉFINITIONS ET INTERPRÉTATION

Définitions

2. (1) Les définitions qui suivent s'appliquent à la présente loi.

« appareil de transmission » *"transmission apparatus"*

« appareil de transmission » Appareil qui appartient à une catégorie réglementaire et dont les fonctions principales sont comprises parmi les suivantes :

a) commutation ou routage de communications;

b) saisie, réception, mise en mémoire, classement, modification, récupération ou sortie de communications, ou tout autre traitement de celles-ci;

c) commande de la vitesse, du code, du protocole, du contenu, de la forme, de la commutation, du routage ou des aspects analogues de communications;

d) toute fonction semblable à celles énumérées aux alinéas *a*) à *c*).

"prescribed" *Version anglaise seulement*

"prescribed" means prescribed by the regulations.

"telecommunications data" *« données de télécommunication »*

"telecommunications data" means data relating to the telecommunications functions of dialling, routing, addressing or signalling 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 or the type of telecommunications service used and includes any information that may be obtained under subsection 492.2(1) of the *Criminal Code*.

"telecommunications facility" *« installation de télécommunication »*

"telecommunications facility" means any facility, apparatus or other thing that is used for telecommunications or for any operation directly connected with telecommunications.

"telecommunications service" *« service de télécommunication »*

"telecommunications service" means a service, or a feature of a service, that is provided by means of telecommunications facilities, whether the provider owns, leases or has any other interest in or right respecting the telecommunications facilities and any related equipment used to provide the service.

"telecommunications service provider" *« télécommunicateur »*

"telecommunications service provider" means a person that, independently or as part of a group or association, provides telecommunications services.

"transmission apparatus" *« appareil de transmission »*

"transmission apparatus" means any apparatus of a prescribed class whose principal functions are one or more of the following:

(*a*) the switching or routing of communications;

(*b*) the input, capture, storage, organization, modification, retrieval, output or other processing of communications;

(*c*) the control of the speed, code, protocol, content, format, switching or routing or similar aspects of communications; or

(*d*) any other function that is similar to one described in paragraphs (*a*) to (*c*).

« autorisée » Se dit de toute personne qui est autorisée, au titre du *Code criminel* ou de la *Loi sur le Service canadien du renseignement de sécurité*, à intercepter des communications. « autorisée » *"authorized"*

« communication » Communication effectuée par voie de télécommunication, y compris les données de télécommunication connexes et toute autre information accessoire. « communication » *"communication"*

« données de télécommunication » Données concernant les fonctions de composition, de routage, d'adressage ou de signalisation en matière de télécommunication et indiquant, ou visant à indiquer, l'origine, le type, la direction, la date, l'heure, la durée, le volume, la destination ou la terminaison de la télécommunication produite ou reçue au moyen d'une installation de télécommunication ou le type de service utilisé. Sont également visés les renseignements obtenus au titre du paragraphe 492.2(1) du *Code criminel*. « données de télécommunication » *"telecommunications data"*

« installation de télécommunication » Installation, appareil ou dispositif quelconque servant à la télécommunication ou à toute opération qui y est directement liée. « installation de télécommunication » *"telecommunications facility"*

« intercepter » S'entend notamment du fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet. « intercepter » *"intercept"*

« ministre » Le ministre de la Sécurité publique et de la Protection civile. « ministre » *"Minister"*

« personne » Sont assimilés à des personnes les sociétés de personnes, les organisations non personnalisées et les administrations et organismes publics. Est assimilée à la personne intéressée toute autre personne ou toute entité qui agit en son nom ou pour elle. « personne » *"person"*

« service de télécommunication » Service — ou complément de service — fourni au moyen d'installations de télécommunication, que celles-ci et le matériel connexe appartiennent au télécommunicateur ou soient loués ou fassent l'objet d'un intérêt ou d'un droit en faveur de celui-ci. « service de télécommunication » *"telecommunications service"*

« télécommunicateur » Personne qui fournit des services de télécommunication, seule ou au titre de son appartenance à un groupe ou à une association.

« télécommunicateur » "*telecommunications service provider*"

Preservation of existing powers

(2) Nothing in this Act derogates from any power in the *Criminal Code*, the *Canadian Security Intelligence Service Act* or the *National Defence Act* to intercept communications or to request that telecommunications service providers assist in such interceptions.

(2) La présente loi ne porte pas atteinte aux pouvoirs prévus par le *Code criminel*, la *Loi sur le Service canadien du renseignement de sécurité* et la *Loi sur la défense nationale* concernant l'interception de toute communication ou toute demande d'assistance adressée aux télécommunicateurs en vue de procéder à une telle interception.

Précision

PURPOSE

OBJET DE LA LOI

Purpose

3. The purpose of this Act is to ensure that telecommunications service providers have the capability to enable national security and law enforcement agencies to exercise their authority to intercept communications and to require telecommunications service providers to provide subscriber and other information, without unreasonably impairing the privacy of individuals, the provision of telecommunications services to Canadians or the competitiveness of the Canadian telecommunications industry.

3. La présente loi a pour objet d'exiger des télécommunicateurs qu'ils disposent des moyens nécessaires pour permettre aux organismes chargés de la sécurité nationale ou du contrôle d'application des lois d'exercer leur pouvoir d'intercepter les communications et qu'ils fournissent des renseignements, notamment sur les abonnés, sans toutefois porter atteinte indûment à la vie privée des particuliers ou entraver sérieusement la prestation de services de télécommunication aux Canadiens et la compétitivité de l'industrie canadienne des télécommunications.

Objet

HER MAJESTY

SA MAJESTÉ

Act binding on Her Majesty

4. This Act is binding on Her Majesty in right of Canada or of a province.

4. La présente loi lie Sa Majesté du chef du Canada et des provinces.

Obligation de Sa Majesté

APPLICATION

CHAMP D'APPLICATION

Exclusions — Schedule 1

5. (1) This Act does not apply to telecommunications service providers in respect of the telecommunications services specified in Part 1 of Schedule 1 or to the telecommunications service providers in the classes listed in Part 2 of that Schedule in respect of the activities specified in that Part for that class.

5. (1) La présente loi ne s'applique pas aux télécommunicateurs à l'égard des services de télécommunication prévus à la partie 1 de l'annexe 1 ni aux télécommunicateurs appartenant aux catégories figurant à la partie 2 de cette annexe à l'égard des activités qui y sont précisées.

Non-application — annexe 1

Partial application — Schedule 2, Part 1

(2) This Act — other than sections 8, 9, 14, 15, 24 to 26, 28 and 32 to 64 — does not apply to the telecommunications service provid- ers in the classes listed in Part 1 of Schedule 2 in respect of the activities specified in that Part for that class.

(2) La présente loi, à l'exception des articles 8, 9, 14, 15, 24 à 26, 28 et 32 à 64, ne s'applique pas aux télécommunicateurs appartenant aux catégories figurant à la partie 1 de l'annexe 2 à l'égard des activités qui y sont précisées.

Application partielle — annexe 2, partie 1

Partial application — Schedule 2, Part 2

(3) This Act, other than section 24, does not apply to the telecommunications service providers in the classes listed in Part 2 of Schedule 2 in respect of the activities specified in that Part for that class.

Application partielle — annexe 2, partie 2

(3) La présente loi, à l'exception de l'article 24, ne s'applique pas aux télécommunicateurs appartenant aux catégories figurant à la partie 2 de l'annexe 2 à l'égard des activités qui y sont précisées.

Amendment of Schedules

(4) The Governor in Council may, by regulation, amend Schedule 1 or 2 by adding, deleting or changing a telecommunications service, an activity or a class of telecommunications service providers.

Modification des annexes

(4) Le gouverneur en conseil peut, par règlement, modifier les annexes 1 et 2 pour y ajouter, en retrancher ou y modifier des services de télécommunication, des activités ou des catégories de télécommunicateurs.

OBLIGATIONS

OBLIGATIONS CONCERNING INTERCEPTIONS

Obligation to have capabilities

6. (1) For the purpose of enabling authorized persons to exercise their authority to intercept communications, every telecommunications service provider must have the capability to do the following:

(*a*) provide intercepted communications to authorized persons; and

(*b*) provide authorized persons with the prescribed information that is in the possession or control of the service provider respecting the location of equipment used in the transmission of communications.

Confidentiality and security measures

(2) A telecommunications service provider, in connection with the interception of communications, must comply with any prescribed confidentiality or security measures.

Obligations for treated communications

(3) If an intercepted communication is encoded, compressed, encrypted or otherwise treated by a telecommunications service provider, the service provider must use the means in its control to provide the intercepted communication in the same form as it was before the communication was treated by the service provider.

Exceptions

(4) Despite subsection (3), a telecommunications service provider is not required to make the form of an intercepted communication the same as it was before the communication was treated if

(*a*) the service provider would be required to develop or acquire decryption techniques or decryption tools; or

OBLIGATIONS

OBLIGATIONS CONCERNANT LES INTERCEPTIONS

Obligations relatives aux mesures de facilitation

6. (1) Afin de permettre à toute personne autorisée d'exercer son pouvoir d'intercepter les communications, il incombe à tout télécommunicateur de disposer des moyens nécessaires pour fournir à celle-ci :

a) toute communication interceptée;

b) toute information réglementaire qu'il a en sa possession ou à sa disposition relativement à l'emplacement de l'équipement utilisé pour la transmission d'une communication.

Confidentialité et sécurité

(2) Le télécommunicateur est tenu d'appliquer les mesures réglementaires concernant la confidentialité et la sécurité pour ce qui est de l'interception de communications.

Traitement de la communication

(3) Si la communication interceptée a fait l'objet d'un traitement — notamment codage, compression et chiffrement — par le télécommunicateur, celui-ci est tenu d'utiliser les moyens dont il dispose pour fournir la communication dans la forme où elle était avant ce traitement.

Exceptions

(4) Il n'est toutefois pas tenu de remettre la communication interceptée dans la forme où elle était avant le traitement dans les cas suivants :

a) il aurait à développer ou à acquérir des méthodes ou des outils de déchiffrement;

(*b*) the treatment is intended only for the purposes of generating a digital signature or for certifying a communication by a prescribed certification authority, and has not been used for any other purpose.

b) le traitement visait uniquement à générer une signature numérique ou à faire certifier la communication par une autorité de certification réglementaire et n'a pas été utilisé à d'autres fins.

Providing information as requested

(5) A telecommunications service provider that is capable of providing intercepted communications to an authorized person in more than one form or manner that conforms with the regulations must provide them in whichever of those forms or manners the authorized person requires.

(5) Il incombe au télécommunicateur, dans le cas où il est en mesure de fournir à la personne autorisée la communication interceptée sous différentes formes et par différents moyens qui sont conformes aux règlements, de la lui fournir dans la forme et par le moyen qu'elle précise.

Fourniture de la communication interceptée

Operational requirements for transmission apparatus

7. The operational requirements in respect of any transmission apparatus are that the telecommunications service provider operating the apparatus have the capability to do the following:

7. Constituent des exigences opérationnelles liées à tout appareil de transmission le fait pour le télécommunicateur qui exploite l'appareil d'être en mesure de prendre les dispositions suivantes :

Exigences opérationnelles liées aux appareils de transmission

(*a*) enable the interception of communications generated by or transmitted through the apparatus to or from any temporary or permanent user of the service provider's telecommunications services;

a) permettre l'interception de la communication produite par l'appareil ou transmise ou reçue au moyen de celui-ci par l'utilisateur temporaire ou permanent de ses services de télécommunication;

(*b*) isolate the communication that is authorized to be intercepted from other information, including

b) isoler la communication dont l'interception est autorisée de toute autre information, notamment isoler :

(i) isolating the communications of the person whose communications are authorized to be intercepted from those of other persons, and

(i) les communications de la personne visée de celles de toute autre personne,

(ii) isolating the telecommunications data of the person whose communications are authorized to be intercepted from the rest of the person's communications;

(ii) les données de télécommunication du reste de ses communications;

(*c*) provide prescribed information that permits the accurate correlation of all elements of intercepted communications; and

c) fournir l'information réglementaire qui permet de mettre en corrélation avec exactitude tous les éléments des communications interceptées;

(*d*) enable simultaneous interceptions by authorized persons from multiple national security and law enforcement agencies of communications of multiple users, including enabling

d) permettre à des personnes autorisées provenant de plusieurs organismes chargés de la sécurité nationale ou du contrôle d'application des lois d'intercepter simultanément des communications de plusieurs utilisateurs, notamment permettre :

(i) at least the minimum number of those interceptions, and

(i) au moins le nombre minimal d'interceptions simultanées,

(ii) any greater number of those interceptions — up to the maximum number — for the period that an agency requests.

(ii) un nombre accru d'interceptions — jusqu'à concurrence du nombre maximal — pour la période demandée par un tel organisme.

No degradation of capabilities

8. A telecommunications service provider that meets, in whole or in part, an operational requirement in respect of transmission apparatus that the service provider operates must continue to so meet that operational requirement.

8. Il incombe au télécommunicateur qui satisfait à tout ou partie d'une exigence opérationnelle liée à un appareil de transmission qu'il exploite de continuer d'y satisfaire.

Maintien de la conformité aux exigences opérationnelles

Maintaining capabilities in respect of new services

9. A telecommunications service provider that meets, in whole or in part, an operational requirement in respect of transmission apparatus that the service provider operates in connection with any of the service provider's telecommunications services must meet that operational requirement to the same extent in respect of any new service that the service provider begins to provide using that apparatus.

9. Il incombe au télécommunicateur qui satisfait à tout ou partie d'une exigence opérationnelle liée à un appareil de transmission qu'il exploite afin de fournir des services de télécommunication d'y satisfaire tout autant à l'égard des nouveaux services qu'il fournit au moyen de l'appareil.

Maintien de la capacité à l'égard des nouveaux services

Beginning to operate transmission apparatus

10. (1) A telecommunications service provider that begins to operate any transmission apparatus for the purpose of providing telecommunications services must meet the operational requirements in respect of the apparatus, whether by means of the apparatus itself or by any other means.

10. (1) Le télécommunicateur qui commence à exploiter un appareil de transmission afin de fournir des services de télécommunication est tenu de satisfaire aux exigences opérationnelles liées à l'appareil, au moyen de celui-ci ou autrement.

Exploitation d'appareils de transmission

Acquisition from another provider

(2) Subsection (1) does not apply in respect of transmission apparatus that a telecommunications service provider acquires from another telecommunications service provider and operates in order to continue to provide the same telecommunications service to approximately the same users. However, the acquiring service provider must continue to meet any operational requirements in respect of the transmission apparatus that the service provider from whom it was acquired was obligated to meet.

(2) Le paragraphe (1) ne s'applique pas si le télécommunicateur commence à exploiter un appareil de transmission qu'il acquiert d'un autre télécommunicateur afin de continuer à fournir les mêmes services de télécommunication à approximativement les mêmes utilisateurs. Toutefois, il est tenu de satisfaire aux mêmes exigences opérationnelles liées à l'appareil que celles auxquelles l'autre télécommunicateur devait satisfaire.

Transfert de propriété

New software

11. (1) When a telecommunications service provider installs new software for any transmission apparatus that the service provider operates, the service provider must meet the operational requirements in respect of that apparatus to the extent that would be enabled by the installation of the software in the form available from the software's manufacturer that would most increase the service provider's ability to meet those operational requirements.

11. (1) Lorsqu'il installe un nouveau logiciel pour un appareil de transmission qu'il exploite, le télécommunicateur est tenu de satisfaire aux exigences opérationnelles liées à l'appareil dans la même mesure que s'il installait le logiciel dans la forme offerte par le fabricant la plus susceptible d'accroître sa capacité de satisfaire à ces exigences.

Installation d'un nouveau logiciel

Other software licences or telecommunications facilities

(2) Subsection (1) applies even if the form of the software in question would require the telecommunications service provider to acquire additional software licences or telecommunications facilities to achieve that increased ability.

(2) Le paragraphe (1) s'applique même si la forme du logiciel, pour qu'elle puisse permettre au télécommunicateur d'accroître ainsi sa capacité, nécessitait l'acquisition de licences d'exploitation ou d'installations de télécommunication supplémentaires.

Licence et installation de télécommunication supplémentaires

Global limit

12. Subject to section 14, a telecommunications service provider is not required, under sections 8 to 11, to increase the service provider's capability to enable simultaneous interceptions beyond the applicable global limit.

12. Sous réserve de l'article 14, le télécommunicateur n'est pas tenu, au titre des articles 8 à 11, d'augmenter sa capacité de permettre des interceptions simultanées au-delà de la limite globale applicable.

Limite globale

Order suspending obligations

13. (1) The Minister may, by order made on the application of a telecommunications service provider, suspend in whole or in part any obligation of the service provider to meet an operational requirement that would arise from the operation of section 10 or 11.

13. (1) Sur demande de tout télécommunicateur, le ministre peut, par arrêté, suspendre en tout ou en partie l'obligation de satisfaire aux exigences opérationnelles découlant de l'application des articles 10 et 11.

Demande de suspension d'obligation

Applications

(2) The application must

(*a*) specify the operational requirement with respect to which an order is sought;

(*b*) set out the reasons for making the application;

(*c*) include a plan that

(i) sets out the measures by which and the time within which the telecommunications service provider proposes to meet the operational requirement specified in accordance with paragraph (*a*),

(ii) describes any measures that the service provider proposes to take to improve the service provider's capability to meet the operational requirements, even if they are not yet applicable, and

(iii) identifies the stages at which and methods by which the Minister can measure progress in the implementation of the plan and the time, manner and form for reports the service provider proposes to make to the Minister; and

(*d*) conform with the prescribed requirements relating to the content or form of the application or the manner in which it is to be made.

(2) La demande :

a) précise les exigences opérationnelles qui sont visées;

b) énonce les moyens sur lesquels elle est fondée;

c) comporte un plan précisant :

(i) les mesures que se propose de prendre le télécommunicateur pour satisfaire à ces exigences opérationnelles et le délai dans lequel il compte le faire,

(ii) les mesures que le télécommunicateur se propose de prendre pour accroître sa capacité de satisfaire aux exigences opérationnelles même si celles-ci ne lui sont pas encore applicables,

(iii) les étapes de sa mise en oeuvre auxquelles le ministre pourra mesurer les progrès réalisés à cet égard, les méthodes pour ce faire, ainsi que les modalités — de temps et autres — concernant les rapports que le télécommunicateur se propose de soumettre au ministre;

d) satisfait aux exigences réglementaires visant son contenu et les modalités de présentation.

Contenu de la demande

Considerations

(3) In deciding whether to make an order, the Minister must take into account the public interest in national security and law enforcement and the commercial interests of the telecommunications service provider as well as any other matter that the Minister considers relevant.

(3) Avant de statuer sur la demande, le ministre prend en considération tous les facteurs qu'il estime pertinents, notamment l'intérêt public — sécurité nationale et contrôle d'application des lois — et les intérêts commerciaux de l'auteur de la demande.

Facteurs à prendre en considération

Notification of decision

(4) The Minister must, within 120 days after the day on which the Minister receives the application, notify the applicant of the Minister's decision to accept or refuse it and, if no notification has been received by the applicant at the end of that period, the Minister is deemed to have refused the application.

(4) Le ministre a cent vingt jours, après la réception de la demande, pour l'accepter ou la refuser; si le télécommunicateur n'est pas avisé de la décision du ministre dans ce délai, celui-ci est réputé avoir refusé.

Notification de la décision

Conditions and term of order

(5) In the order, the Minister may include any conditions that the Minister considers appropriate and must fix its term for a period of not more than three years.

(5) Le ministre peut, dans l'arrêté, assortir la suspension des conditions qu'il estime indiquées et l'accorde pour une période maximale de trois ans.

Conditions et durée de la suspension

Obligation to comply with conditions of order

(6) The telecommunications service provider must comply with the conditions of the order as soon as the service provider begins to operate the telecommunications apparatus or installs the new software, as the case may be.

(6) Le télécommunicateur est tenu de satisfaire à de telles conditions dès qu'il commence à exploiter l'appareil de transmission en cause ou qu'il installe le nouveau logiciel.

Obligation de satisfaire aux conditions imposées par le ministre

Notice of revocation

(7) The Minister may revoke an order on written notice to the telecommunications service provider if

(*a*) the service provider has contravened this Act, the regulations or the conditions of the order; or

(*b*) the order was obtained through misrepresentation.

(7) Le ministre peut, sur avis écrit donné au télécommunicateur, révoquer l'arrêté :

a) soit au motif que celui-ci a enfreint la présente loi, ses règlements ou les conditions de la suspension;

b) soit au motif que la suspension a été obtenue par des moyens faux ou trompeurs.

Avis de révocation

Amendment

(8) The Minister may amend an order with the consent of the telecommunications service provider.

(8) Il peut modifier l'arrêté avec le consentement du télécommunicateur.

Modification

Ministerial orders

14. (1) The Minister may, at the request of the Commissioner of the Royal Canadian Mounted Police or the Director of the Canadian Security Intelligence Service and if in the Minister's opinion it is necessary to do so, order a telecommunications service provider

(*a*) to comply with any obligation under subsections 6(1) and (2) in a manner or within a time that the Minister specifies;

(*b*) to enable, in a manner or within a time that the Minister specifies, a number of simultaneous interceptions greater than any maximum or limit that would otherwise apply;

(*c*) to comply, in a manner or within a time that the Minister specifies, with any confidentiality or security measures respecting

14. (1) S'il le juge nécessaire, le ministre peut par arrêté, à la demande du commissaire de la Gendarmerie royale du Canada ou du directeur du Service canadien du renseignement de sécurité, ordonner au télécommunicateur :

a) d'exécuter, selon les modalités — de temps et autres — indiquées, toute obligation prévue aux paragraphes 6(1) et (2);

b) de permettre, selon les modalités — de temps et autres — indiquées, de faire des interceptions simultanées en un nombre supérieur à la limite qui s'appliquerait par ailleurs;

c) d'appliquer, selon les modalités — de temps et autres — indiquées, des mesures concernant la confidentialité ou la sécurité liées aux interceptions qui s'ajoutent à celles visées au paragraphe 6(2);

Arrêté

interceptions that the Minister specifies in addition to those referred to in subsection 6(2);

(*d*) to meet an operational requirement in respect of transmission apparatus operated by the service provider that the service provider would not otherwise be required to meet; or

(*e*) to meet an operational requirement in respect of transmission apparatus operated by the service provider in a manner or within a time that the Minister specifies.

d) de satisfaire à toute exigence opérationnelle qui ne lui est pas par ailleurs applicable et qui est liée à un appareil de transmission qu'il exploite;

e) de satisfaire, selon les modalités — de temps et autres — indiquées, à toute exigence opérationnelle liée à un appareil de transmission qu'il exploite.

Limitation

(2) The Minister is not authorized to make an order under subsection (1) in respect of a telecommunications service provider in relation to a telecommunications service specified in Part 1 of Schedule 1 or in respect of a telecommunications service provider in a class listed in Part 2 of Schedule 1 or Part 2 of Schedule 2 in relation to the activities specified for that class in Part 2 of Schedule 1 or Part 2 of Schedule 2, as the case may be.

Limite

(2) Il ne peut toutefois prendre d'arrêté en vertu du paragraphe (1) à l'égard des télécommunicateurs relativement aux services de télécommunication prévus à la partie 1 de l'annexe 1 ni à l'égard des télécommunicateurs appartenant aux catégories figurant à la partie 2 de cette annexe ou à la partie 2 de l'annexe 2 relativement aux activités qui y sont précisées.

Compensation

(3) The Commissioner of the Royal Canadian Mounted Police or the Director of the Canadian Security Intelligence Service, as the case may be, must pay the telecommunications service provider an amount that the Minister considers reasonable towards the expenses that the Minister considers are necessary for the service provider to incur initially to comply with an order made under this section.

Indemnisation

(3) Le commissaire de la Gendarmerie royale du Canada ou le directeur du Service canadien du renseignement de sécurité, selon le cas, verse au télécommunicateur l'indemnité que le ministre estime suffisante au regard des dépenses qui, à son avis, sont nécessaires et que le télécommunicateur engage initialement pour se conformer à l'arrêté.

Equipment

(4) The Minister may provide the telecommunications service provider with any equipment or other thing that the Minister considers the service provider needs to comply with an order made under this section.

Équipement

(4) Le ministre peut fournir au télécommunicateur l'équipement et les autres biens qu'il estime nécessaires pour lui permettre de se conformer à l'arrêté.

Non-application of sections 8 and 9

(5) Sections 8 and 9 do not apply in respect of any equipment or other thing provided by the Minister under subsection (4). However, the telecommunications service provider must provide notice to the Minister of any problems with the equipment or other thing provided and provide assistance in resolving the problem.

Non-application des articles 8 et 9

(5) Les articles 8 et 9 ne s'appliquent pas à l'équipement et aux autres biens fournis par le ministre. Toutefois, le télécommunicateur est tenu d'aviser le ministre de tout problème que ceux-ci présentent et de prêter son assistance pour le corriger.

Order prevails

(6) An order made by the Minister under subsection (1) prevails over any regulations, to the extent of any inconsistency.

Incompatibilité

(6) L'arrêté pris en vertu du paragraphe (1) l'emporte sur tout règlement incompatible.

Delegation

(7) The Commissioner of the Royal Canadian Mounted Police and the Director of the Canadian Security Intelligence Service may delegate his or her power to pay amounts under subsection (3) to, respectively, a member of a prescribed class of senior officers of the Royal Canadian Mounted Police or a member of a prescribed class of senior officials of the Canadian Security Intelligence Service.

Délégation

(7) Le commissaire de la Gendarmerie royale du Canada peut déléguer son pouvoir de verser l'indemnité visée au paragraphe (3) à tout membre d'une catégorie réglementaire d'officiers supérieurs de son organisme. Le directeur du Service canadien du renseignement de sécurité peut déléguer son propre pouvoir de verser l'indemnité visée au paragraphe (3) à tout membre d'une catégorie réglementaire de cadres supérieurs de son organisme.

Statutory Instruments Act does not apply

15. The *Statutory Instruments Act* does not apply in respect of an order made under section 13 or 14.

Non-application de la *Loi sur les textes réglementaires*

15. La *Loi sur les textes réglementaires* ne s'applique pas aux arrêtés pris en vertu des articles 13 ou 14.

OBLIGATIONS CONCERNING SUBSCRIBER INFORMATION

OBLIGATIONS CONCERNANT LES RENSEIGNEMENTS SUR LES ABONNÉS

Provision of subscriber information

16. (1) Every telecommunications service provider must provide a person designated under subsection (3), on his or her written request, with any information in the service provider's possession or control respecting the name, address, telephone number and electronic mail address of any subscriber to any of the service provider's telecommunications services and the Internet protocol address, mobile identification number, electronic serial number, local service provider identifier, international mobile equipment identity number, international mobile subscriber identity number and subscriber identity module card number that are associated with the subscriber's service and equipment.

Accès aux renseignements sur les abonnés

16. (1) Le télécommunicateur fournit, sur demande écrite, à toute personne désignée en vertu du paragraphe (3) les renseignements qu'il a en sa possession ou à sa disposition concernant les nom, adresse, numéro de téléphone et adresse de courriel de tout abonné de ses services de télécommunication et l'adresse de protocole Internet, le numéro d'identification mobile, le numéro de série électronique, l'identificateur du fournisseur de services locaux, le numéro d'identité international d'équipement mobile, le numéro d'identité internationale d'abonné mobile ainsi que le numéro de module d'identité d'abonné de service associés aux services et à l'équipement de l'abonné.

Purpose of the request

(2) A designated person must ensure that he or she makes a request under subsection (1) only in performing, as the case may be, a duty or function

(*a*) of the Canadian Security Intelligence Service under the *Canadian Security Intelligence Service Act*;

(*b*) of a police service, including any related to the enforcement of any laws of Canada, of a province or of a foreign jurisdiction; or

(*c*) of the Commissioner of Competition under the *Competition Act*.

Objet de la demande

(2) La personne désignée veille à ce que la demande ne soit faite que dans l'exercice d'une fonction, selon le cas :

a) du Service canadien du renseignement de sécurité au titre de la *Loi sur le Service canadien du renseignement de sécurité*;

b) d'un service de police, notamment en ce qui a trait au contrôle d'application du droit canadien, provincial ou étranger;

c) du commissaire de la concurrence au titre de la *Loi sur la concurrence*.

Designated persons

(3) The Commissioner of the Royal Canadian Mounted Police, the Director of the Canadian Security Intelligence Service, the

Personnes désignées

(3) Pour l'application du présent article, le commissaire de la Gendarmerie royale du Canada, le directeur du Service canadien du

Commissioner of Competition and the chief or head of a police service constituted under the laws of a province may designate for the purposes of this section any employee of his or her agency, or a class of such employees, whose duties are related to protecting national security or to law enforcement.

renseignement de sécurité, le commissaire de la concurrence ou le chef ou directeur d'un service de police constitué sous le régime d'une loi provinciale peut désigner, nommément ou par catégorie, les employés de son organisme dont les fonctions sont liées à la protection de la sécurité nationale ou au contrôle d'application des lois.

Limit on number of designated persons

(4) The number of persons designated under subsection (3) in respect of a particular agency may not exceed the greater of five and the number that is equal to five per cent of the total number of employees of that agency.

(4) Le nombre de personnes désignées par organisme ne peut dépasser cinq ou, s'il est supérieur, le nombre correspondant à cinq pour cent des effectifs.

Limite du nombre de personnes désignées

Delegation

(5) The Commissioner of the Royal Canadian Mounted Police and the Director of the Canadian Security Intelligence Service may delegate his or her power to designate persons under subsection (3) to, respectively, a member of a prescribed class of senior officers of the Royal Canadian Mounted Police or a member of a prescribed class of senior officials of the Canadian Security Intelligence Service.

(5) Le commissaire de la Gendarmerie royale du Canada peut déléguer son pouvoir de désignation à tout membre d'une catégorie réglementaire d'officiers supérieurs de son organisme. Le directeur du Service canadien du renseignement de sécurité peut déléguer son propre pouvoir de désignation à tout membre d'une catégorie réglementaire de cadres supérieurs de son organisme.

Délégation

Exceptional circumstances

17. (1) A police officer may request a telecommunications service provider to provide the officer with the information referred to in subsection 16(1) in the following circumstances:

(*a*) the officer believes on reasonable grounds that the urgency of the situation is such that the request cannot, with reasonable diligence, be made under that subsection;

(*b*) the officer believes on reasonable grounds that the information requested is immediately necessary to prevent an unlawful act that would cause serious harm to any person or to property; and

(*c*) the information directly concerns either the person who would perform the act that is likely to cause the harm or is the victim, or intended victim, of the harm.

The police officer must inform the telecommunications service provider of his or her name, rank, badge number and the agency in which he or she is employed and state that the request is being made in exceptional circumstances and under the authority of this subsection.

17. (1) Tout officier de police peut demander au télécommunicateur de lui fournir les renseignements visés au paragraphe 16(1) si, à la fois :

a) il a des motifs raisonnables de croire que l'urgence de la situation est telle qu'une demande ne peut, avec toute la diligence voulue, être faite en vertu de ce paragraphe;

b) il a des motifs raisonnables de croire que les renseignements demandés sont immédiatement nécessaires pour empêcher la perpétration d'un acte illicite qui causerait des blessures corporelles graves ou des dommages importants à un bien;

c) les renseignements portent directement sur soit la personne dont les actes sont susceptibles de causer les blessures ou les dommages, soit la victime ou la personne menacée.

Il communique au télécommunicateur ses nom, rang et numéro d'insigne ainsi que le nom de son organisme et l'informe que la demande est faite en vertu du présent paragraphe en raison de circonstances exceptionnelles.

Circonstances exceptionnelles

Obligation of telecommunications service provider

(2) The telecommunications service provider must provide the information to the police officer as if the request were made by a designated person under subsection 16(1).

(2) Le télécommunicateur lui fournit les renseignements demandés comme si la demande avait été faite en vertu du paragraphe 16(1) par une personne désignée.

Obligation du télécommunicateur

Communication

(3) The police officer must, within 24 hours after making a request under subsection (1), communicate to a designated person employed in the same agency as the officer all of the information relating to the request that would be necessary if it had been made under subsection 16(1) and inform that person of the circumstances referred to in paragraphs (1)(*a*) to (*c*).

(3) Dans les vingt-quatre heures suivant la présentation de sa demande, l'officier de police transmet à toute personne désignée relevant de son organisme l'information concernant la demande qui aurait été nécessaire si celle-ci avait été faite en vertu du paragraphe 16(1) et l'informe des circonstances visées aux alinéas (1)*a*) à *c*).

Transmission d'information

Notice

(4) On receiving the information, the designated person must in writing inform the telecommunications service provider that the request was made in exceptional circumstances under the authority of subsection (1).

(4) Sur réception de l'information, la personne désignée informe par écrit le télécommunicateur du fait que la demande a été faite en vertu du paragraphe (1) en raison de circonstances exceptionnelles.

Avis

Creation of record by designated person

18. (1) A designated person who makes a request under subsection 16(1), or who receives information under subsection 17(3), must create a record that

(*a*) in the case of a request under subsection 16(1), identifies the duty or function referred to in subsection 16(2) in the performance of which the request is made, describes the relevance of the information requested to that duty or function and includes any other information that justifies the request and any other prescribed information; and

(*b*) in the case where the designated person receives information under subsection 17(3), includes the information referred to in paragraph (*a*) as well as the circumstances referred to in paragraphs 17(1)(*a*) to (*c*).

18. (1) La personne désignée qui fait une demande en vertu du paragraphe 16(1) ou qui reçoit de l'information au titre du paragraphe 17(3) est tenue de créer un registre faisant état de ce qui suit :

a) dans le cas où elle a fait la demande, la fonction visée au paragraphe 16(2) dans l'exercice de laquelle elle l'a faite et la pertinence des renseignements demandés en regard de l'exercice de cette fonction, ainsi que tout autre justificatif et tout autre renseignement prévus par règlement;

b) dans le cas où elle a reçu l'information, les renseignements visés à l'alinéa *a*) et les circonstances visées aux alinéas 17(1)*a*) à *c*).

Création d'un registre — personne désignée

Retention of records and dealing with information

(2) The agency that employs the designated person must retain records created under subsection (1) and deal with the information provided in response to requests made under subsection 16(1) or 17(1).

(2) L'organisme dont relève la personne désignée est tenu de conserver le registre et de traiter les renseignements obtenus dans le cadre des demandes faites en vertu des paragraphes 16(1) ou 17(1).

Tenue du registre et traitement des renseignements

Use of information

19. Information that is provided in response to a request made under subsection 16(1) or 17(1) must not, without the consent of the individual to whom it relates, be used by the agency in which the designated person or police officer is employed except for the purpose for which the information was obtained or for a use consistent with that purpose.

19. Sauf consentement de l'intéressé, les renseignements obtenus par la personne désignée ou l'officier de police ne peuvent servir à son organisme qu'aux fins auxquelles ils ont été obtenus ou que pour des usages compatibles avec ces fins.

Usage des renseignements recueillis

Internal audit

20. (1) The Commissioner of the Royal Canadian Mounted Police, the Director of the Canadian Security Intelligence Service, the Commissioner of Competition and any chief or head of a police service constituted under the laws of a province who makes a designation under subsection 16(3) must cause internal audits to be regularly conducted of the practices of his or her agency to ensure compliance with sections 16 to 19 and the regulations made for the purposes of those sections and of the internal management and information systems and controls concerning requests made under sections 16 and 17.

Vérification interne

20. (1) Le commissaire de la Gendarmerie royale du Canada, le directeur du Service canadien du renseignement de sécurité, le commissaire de la concurrence ou le chef ou directeur d'un service de police constitué sous le régime d'une loi provinciale qui a fait la désignation prévue au paragraphe 16(3) fait procéder régulièrement, d'une part, à des vérifications internes des méthodes et usages de son organisme afin de contrôler l'observation des articles 16 à 19 et de leurs règlements d'application et, d'autre part, à des vérifications internes des moyens de contrôle et des systèmes en matière de gestion et d'information concernant les demandes prévues aux articles 16 et 17.

Report to responsible minister

(2) The person who causes an internal audit to be conducted must, without delay, make a report to the responsible minister of anything arising out of the audit that in his or her opinion should be brought to the attention of that minister including any corrective action proposed or taken.

Rapport au ministre

(2) La personne qui fait procéder à une vérification interne établit dans les meilleurs délais à l'intention du ministre compétent un rapport sur toute question découlant de la vérification qui, à son avis, doit être portée à la connaissance de celui-ci, y compris les mesures de redressement prises ou proposées.

Copy of report

(3) A copy of the report is to be provided by that person

(*a*) if it concerns the Royal Canadian Mounted Police or the Commissioner of Competition, to the Privacy Commissioner appointed under section 53 of the *Privacy Act*;

(*b*) if it concerns the Canadian Security Intelligence Service, to the Security Intelligence Review Committee established by subsection 34(1) of the *Canadian Security Intelligence Service Act*; and

(*c*) if it concerns a police service constituted under the laws of a province, to the public officer for that province whose duties include investigations relating to the protection of privacy.

Copie du rapport

(3) Elle transmet une copie du rapport :

a) si celui-ci est établi par le commissaire de la Gendarmerie royale du Canada ou le commissaire de la concurrence, au Commissaire à la protection de la vie privée nommé en vertu de l'article 53 de la *Loi sur la protection des renseignements personnels*;

b) s'il est établi par le directeur du Service canadien du renseignement de sécurité, au comité de surveillance des activités de renseignement de sécurité constitué par le paragraphe 34(1) de la *Loi sur le Service canadien du renseignement de sécurité*;

c) s'il est établi par le chef ou directeur d'un service de police constitué sous le régime d'une loi provinciale, au fonctionnaire de la province dont les fonctions comportent les enquêtes relatives à la protection de la vie privée.

Audit — Privacy Commissioner

(4) The Privacy Commissioner may, on reasonable notice, conduct an audit of the practices of the Royal Canadian Mounted Police or the Commissioner of Competition to ensure compliance with sections 16 to 19 and the regulations made for the purposes of those

Vérification : Commissaire à la protection de la vie privée

(4) Le Commissaire à la protection de la vie privée peut, sur préavis suffisant, procéder, d'une part, à des vérifications des méthodes et usages de la Gendarmerie royale du Canada ou du commissaire de la concurrence afin de contrôler l'observation des articles 16 à 19 et

sections and of the internal management and information systems and controls concerning requests made under sections 16 and 17. The provisions of the *Privacy Act* apply, with any necessary modifications, in respect of the audit as if it were an investigation under that Act.

de leurs règlements d'application et, d'autre part, à des vérifications des moyens de contrôle et des systèmes en matière de gestion et d'information de l'un ou l'autre concernant les demandes prévues aux articles 16 et 17. La *Loi sur la protection des renseignements personnels* s'applique, avec les adaptations nécessaires, à la vérification comme si elle constituait une enquête en vertu de cette loi.

Audit — Security Intelligence Review Committee

(5) For greater certainty, the functions of the Security Intelligence Review Committee under section 38 of the *Canadian Security Intelligence Service Act* include the power to conduct an audit of the practices of the Canadian Security Intelligence Service to ensure compliance with sections 16, 18 and 19 and the regulations made for the purposes of those sections and of the internal management and information systems and controls concerning requests made under section 16.

(5) Il est entendu que les fonctions du comité de surveillance des activités de renseignement de sécurité prévues à l'article 38 de la *Loi sur le Service canadien du renseignement de sécurité* comportent le pouvoir de procéder aux vérifications des méthodes et usages du Service canadien du renseignement de sécurité afin de contrôler l'observation des articles 16, 18 et 19 et de leurs règlements d'application et aux vérifications des moyens de contrôle et des systèmes en matière de gestion et d'information de celui-ci concernant les demandes prévues à l'article 16.

Vérification : comité de surveillance des activités de renseignement de sécurité

Report concerning provincial audit capability

(6) The Privacy Commissioner must, in the report made to Parliament for each financial year, identify the public officers to whom copies of reports are to be provided under paragraph (3)(*c*) and report on the powers that they have to conduct audits similar to those referred to in subsection (4) with respect to the police services constituted under the laws of their province.

(6) Le Commissaire à la protection de la vie privée fait état, dans le rapport qu'il présente pour chaque exercice au Parlement, des fonctionnaires à qui des rapports doivent être transmis en application de l'alinéa (3)*c*) et du pouvoir qu'ils possèdent de procéder à des vérifications semblables à celles visées au paragraphe (4) à l'égard des services de police constitués sous le régime des lois de leur province.

Rapport concernant la vérification faite au niveau provincial

Records of service provider

(7) A person conducting an internal audit under this section may require a telecommunications service provider to give the person access to any records in the possession or control of the service provider that are relevant to the audit.

(7) Toute personne procédant à une vérification interne au titre du présent article peut exiger de tout télécommunicateur qu'il lui donne accès à tout registre qu'il possède ou dont il dispose et qui est pertinent.

Registres des télécommunicateurs

Definition of "responsible minister"

(8) For the purposes of this section, "responsible minister" means

(*a*) in relation to the Commissioner of the Royal Canadian Mounted Police and the Director of the Canadian Security Intelligence Service, the Minister of Public Safety and Emergency Preparedness;

(*b*) in relation to the Commissioner of Competition, the Minister of Industry; and

(8) Pour l'application du présent article, « ministre compétent » s'entend :

a) s'agissant du commissaire de la Gendarmerie royale du Canada et du directeur du Service canadien du renseignement de sécurité, du ministre de la Sécurité publique et de la Protection civile;

b) s'agissant du commissaire de la concurrence, du ministre de l'Industrie;

Définition de « ministre compétent »

(*c*) in relation to the chief or head of a police service constituted under the laws of a province, the Attorney General of that province.

c) s'agissant du chef ou directeur d'un service de police constitué sous le régime d'une loi provinciale, du procureur général de la province.

Entitlement to fee

21. (1) A telecommunications service provider that provides information to a person under section 16 or 17 is entitled to be paid the prescribed fee for providing the information.

21. (1) Le télécommunicateur qui fournit des renseignements en application des articles 16 ou 17 a le droit de recevoir les droits réglementaires.

Droits

Payment of fee by designating authority

(2) If the information is requested by a designated person under section 16, the fee is to be paid by the designating authority.

(2) Si la demande est faite par une personne désignée au titre de l'article 16, les droits sont payés par la personne qui l'a désignée.

Paiement des droits— personne désignée

Payment of fee by police service

(3) If the information is requested by a police officer under section 17, the fee is to be paid by the chief or head of the police service that employs the police officer.

(3) Si elle est faite par un officier de police au titre de l'article 17, ils sont payés par le chef ou directeur du service de police de qui relève l'officier.

Paiement des droits— officier de police

Preservation of existing authority

22. Nothing in this Act derogates from any other authority under law to obtain the information referred to in subsection 16(1) from a telecommunications service provider.

22. La présente loi n'a pas pour effet de porter atteinte aux pouvoirs de quiconque d'obtenir, en application d'une règle de droit, les renseignements visés au paragraphe 16(1) auprès d'un télécommunicateur.

Précision

Deemed nature of information

23. Personal information, as defined in subsection 2(1) of the *Personal Information Protection and Electronic Documents Act*, that is provided under subsection 16(1) or 17(1) is deemed, for the purposes of subsections 9(2.1) to (2.4) of that Act, to be disclosed under subparagraph 7(3)(*c.1*)(i) or (ii), and not under paragraph 7(3)(*i*), of that Act. This section operates despite the other provisions of Part 1 of that Act.

23. Pour l'application des paragraphes 9(2.1) à (2.4) de la *Loi sur la protection des renseignements personnels et les documents électroniques*, les renseignements personnels au sens du paragraphe 2(1) de cette loi qui sont fournis au titre des paragraphes 16(1) ou 17(1) sont réputés être communiqués au titre des sous-alinéas 7(3)*c.1*)(i) ou (ii) de cette loi et non de son alinéa 7(3)*i*). Le présent article s'applique malgré les autres dispositions de la partie 1 de la même loi.

Dérogation

MISCELLANEOUS PROVISIONS

DISPOSITIONS DIVERSES

Facility and service information

24. (1) A telecommunications service provider must, on the request of a police officer or of an employee of the Royal Canadian Mounted Police or the Canadian Security Intelligence Service,

(*a*) provide the prescribed information relating to the service provider's telecommunications facilities;

(*b*) indicate what telecommunications services the service provider offers to subscribers; and

24. (1) Sur demande de tout officier de police ou employé de la Gendarmerie royale du Canada ou du Service canadien du renseignement de sécurité, le télécommunicateur :

a) lui fournit l'information réglementaire se rapportant à ses installations de télécommunication;

b) lui indique la nature des services de télécommunication qu'il offre à ses abonnés;

Renseignements sur les installations et les services

(*c*) provide the name, address and telephone number of any telecommunications service providers from whom the service provider obtains or to whom the service provider provides telecommunications services, if the service provider has that information.

c) lui fournit les nom, adresse et numéro de téléphone, s'il les connaît, de tout autre télécommunicateur dont il obtient des services de télécommunication ou à qui il en fournit.

Obligation to provide information to authorized persons

(2) A telecommunications service provider must, on the request of an authorized person, provide the prescribed information concerning

(*a*) telecommunications services that are provided by the service provider to a person whose communications are the subject of a court order authorizing their interception; and

(*b*) telecommunications facilities that are used by the service provider in providing those telecommunications services.

Obligation de fournir des renseignements à une personne autorisée

(2) Sur demande de toute personne autorisée, le télécommunicateur lui fournit l'information réglementaire concernant :

a) les services de télécommunication qu'il fournit à la personne dont les communications font l'objet d'une ordonnance judiciaire autorisant leur interception;

b) les installations de télécommunication qu'il utilise pour lui fournir ces services de télécommunication.

Obligation to assist — assessment and testing

25. A telecommunications service provider must, on the request of a police officer or of an employee of the Royal Canadian Mounted Police or the Canadian Security Intelligence Service, provide all reasonable assistance to permit the police officer or employee to assess or to test the service provider's telecommunications facilities that may be used to intercept communications.

Obligation de prêter assistance : évaluation et mise à l'essai

25. Sur demande de tout officier de police ou employé de la Gendarmerie royale du Canada ou du Service canadien du renseignement de sécurité, le télécommunicateur lui prête toute l'assistance possible pour évaluer ou mettre à l'essai celles de ses installations de télécommunication pouvant servir aux interceptions.

Notification of change

26. If the Canadian Security Intelligence Service or a law enforcement agency has provided a telecommunications service provider with any equipment or other thing for intercepting communications, the service provider must, before making any change to the service provider's telecommunications facilities that is likely to impair or reduce the interception capability of the equipment or other thing, notify the Canadian Security Intelligence Service or law enforcement agency, as the case may be, of the change.

Notification

26. Si le Service canadien du renseignement de sécurité ou tout organisme chargé du contrôle d'application des lois lui a fourni tout équipement ou autre bien pouvant servir aux interceptions, le télécommunicateur notifie préalablement au Service ou à l'organisme, selon le cas, toute modification à ses installations qui portera vraisemblablement atteinte à la capacité d'interception de l'équipement ou du bien.

Notification — simultaneous interception capability

27. A telecommunications service provider must notify the Minister when

(*a*) in respect of any particular transmission apparatus, the increased number of simultaneous interceptions that the service provider is required, as a result of a request referred to in subparagraph 7(*d*)(ii), to be capable of enabling is 75% or more of the maximum number that is applicable under that subparagraph; or

Notification : interceptions simultanées

27. Le télécommunicateur informe le ministre lorsque :

a) à l'égard d'un appareil de transmission donné, le nombre accru d'interceptions simultanées qu'il doit être en mesure de permettre par suite de la demande visée au sous-alinéa 7*d*)(ii) atteint 75 % du nombre maximal applicable au titre de ce sous-alinéa;

(*b*) the number of simultaneous interceptions that the service provider is required, under sections 8 to 11, to be capable of enabling is 75% or more of the global limit that is applicable under section 12.

b) le nombre d'interceptions simultanées qu'il doit être en mesure de permettre en application des articles 8 à 11 atteint 75 % de la limite globale applicable au titre de l'article 12.

Persons engaged in interceptions

28. (1) A telecommunications service provider must, on the request of the Royal Canadian Mounted Police or the Canadian Security Intelligence Service, provide a list of the names of the persons who are employed by or carrying out work for the service provider who may assist in the interception of communications.

28. (1) Sur demande de la Gendarmerie royale du Canada ou du Service canadien du renseignement de sécurité, le télécommunicateur lui fournit la liste des noms de ses employés ou contractuels qui peuvent prêter assistance dans le cadre de l'interception d'une communication.

Liste d'employés pouvant prêter assistance

Changes to the list

(2) A telecommunications service provider must provide any changes to the list to the agency who made the request.

(2) Il informe l'organisme qui a fait la demande de toute modification à la liste.

Modification à la liste

Security assessments

(3) The Royal Canadian Mounted Police or the Canadian Security Intelligence Service may conduct an investigation for the purposes of a security assessment of any of those persons who consent to the investigation.

(3) La Gendarmerie royale du Canada ou le Service canadien du renseignement de sécurité peut tenir une enquête en vue d'une évaluation de sécurité de ces employés et contractuels s'ils y consentent.

Évaluation de sécurité

Specialized telecommunications support

29. (1) If the prescribed conditions are met, a telecommunications service provider that provides under this Act prescribed specialized telecommunications support to the Canadian Security Intelligence Service or a law enforcement agency is entitled, on request, to be paid an amount determined in accordance with the regulations for providing that support.

29. (1) Le télécommunicateur qui, au titre de la présente loi, fournit de l'appui spécialisé en télécommunication, prévu par règlement, au Service canadien du renseignement de sécurité ou à tout organisme chargé du contrôle d'application des lois a le droit de recevoir, sur demande, si les conditions réglementaires sont satisfaites, la somme établie conformément aux règlements.

Appui spécialisé en télécommunication

Payment

(2) The amount must be paid by the agency that received the specialized telecommunications support.

(2) La somme est payée par l'organisme qui a reçu l'appui spécialisé en télécommunication.

Paiement

Mandatory reporting — acquisition of transmission apparatus

30. (1) A telecommunications service provider that acquires transmission apparatus referred to in subsection 10(2) must, before using it in providing telecommunications services, submit to the Minister a report in the prescribed form and manner containing the following information:

(*a*) the prescribed information concerning the extent to which the service provider meets operational requirements in respect of the transmission apparatus; and

(*b*) any prescribed information relevant to the administration of this Act.

30. (1) Le télécommunicateur qui acquiert tout appareil de transmission visé au paragraphe 10(2) présente au ministre, avant de fournir des services de télécommunication au moyen de l'appareil, un rapport établi selon les modalités réglementaires et contenant les renseignements suivants :

a) les renseignements réglementaires indiquant la mesure dans laquelle il satisfait aux exigences opérationnelles liées à l'appareil;

b) tout renseignement réglementaire qui touche à l'application de la présente loi.

Rapport : acquisition d'appareil

Other reporting

(2) A telecommunications service provider must, at the request of the Minister, submit a report or further report in the form and manner, and within the period, that the Minister specifies containing the information referred to in paragraphs (1)(*a*) and (*b*) and any additional related information that the Minister specifies.

Autre rapport

(2) Sur demande du ministre, le télécommunicateur présente, selon les modalités de temps et autres précisées, un rapport contenant les renseignements visés aux alinéas (1)*a*) et *b*) et les renseignements complémentaires précisés.

Statement

(3) Every report submitted under this section must include a written statement certifying that it does not contain any untrue statements or omissions of material facts, that it fairly presents the telecommunications service provider's operations at the time of submission and that the signator has taken steps to ensure the report's accuracy and promises to correct any material error that is detected in the report after its submission and to submit a revised report to the Minister as soon as possible, with another similar written statement accompanying it.

Attestation

(3) Le rapport présenté en conformité avec le présent article comprend une attestation portant qu'il ne comporte aucun faux renseignement, qu'il comporte tous les renseignements importants et qu'il présente fidèlement la situation du télécommunicateur à la date de sa présentation. Le signataire atteste également qu'il a pris toutes les mesures nécessaires pour s'assurer de l'exactitude du rapport. Si des erreurs importantes sont découvertes dans le rapport après sa présentation, il s'engage à faire parvenir au ministre, dans les meilleurs délais, un rapport corrigé qui comprend une autre attestation.

Signator of statement

(4) The statement must be signed

(*a*) if the telecommunications service provider is a corporation, by one of its officers or directors; and

(*b*) in any other case, by an individual who is an owner of the telecommunications service provider or by an officer or a director of a corporation that is an owner of the telecommunications service provider.

Signataire

(4) Le signataire de l'attestation est :

a) dans le cas où le télécommunicateur est une personne morale, un de ses dirigeants ou administrateurs;

b) dans les autres cas, soit le particulier qui est propriétaire du télécommunicateur, seul ou avec d'autres, soit un des dirigeants ou administrateurs de la personne morale qui en est propriétaire, seule ou avec d'autres.

No redundant performance required

31. If two or more telecommunications service providers have, in effect, the same obligation under this Act in connection with any given transmission apparatus or a given interception and any one of them performs that obligation, it is deemed to be performed by all.

Exécution d'une obligation

31. Si plusieurs télécommunicateurs sont tenus d'exécuter la même obligation prévue par la présente loi dans le cadre de l'exploitation d'un appareil de transmission ou d'une interception, ils sont solidaires de l'exécution de cette obligation par l'un d'eux.

EXEMPTIONS

EXEMPTIONS

Exemption regulation

32. (1) The Governor in Council may, on the recommendation of the Minister and the Minister of Industry, by regulation, exempt any class of telecommunications service providers from all or part of the obligations under any of sections 6, 9 to 11, 16, 17 and 30 or under any regulations made for the purposes of those sections.

Règlement d'exemption

32. (1) Sur recommandation du ministre et du ministre de l'Industrie, le gouverneur en conseil peut par règlement exempter, par catégorie, des télécommunicateurs de tout ou partie des obligations prévues aux articles 6, 9 à 11, 16, 17 et 30 et par leurs règlements d'application.

Considerations

(2) Before making or amending such a regulation, the Governor in Council must consider

(*a*) the extent to which the exemption would adversely affect national security or law enforcement;

(*b*) whether the telecommunications service providers can comply with the obligations from which they would be exempted;

(*c*) whether the costs of compliance with those obligations would have an unreasonable adverse effect on the business of the telecommunications service providers; and

(*d*) whether compliance with those obligations would unreasonably impair the provision of telecommunications services to Canadians or the competitiveness of the Canadian telecommunications industry.

Éléments à prendre en considération

(2) Avant de prendre ou de modifier un tel règlement, le gouverneur en conseil prend en considération :

a) la mesure dans laquelle l'exemption est susceptible de nuire à la sécurité nationale ou au contrôle d'application des lois;

b) le fait que les télécommunicateurs visés ont la capacité ou non d'exécuter les obligations en cause;

c) le fait que les dépenses liées au respect des obligations en cause auraient ou non des effets négatifs injustifiés sur les activités commerciales des télécommunicateurs;

d) le fait que l'exécution des obligations en cause entraverait ou non sérieusement la prestation de services de télécommunication aux Canadiens ou la compétitivité de l'industrie canadienne des télécommunications.

Conditions and term of regulation

(3) In the regulation, the Governor in Council may include any conditions that the Governor in Council considers appropriate and must fix its term for a period of not more than two years.

Conditions et durée de l'exemption

(3) Il peut assortir l'exemption des conditions qu'il estime indiquées et l'accorde pour une période maximale de deux ans.

Exemptions related to section 10 or 11

(4) When a regulation under which a telecommunications service provider is exempted from an obligation under section 10 or 11 expires or is repealed, section 10 or 11, as the case may be, applies to the telecommunications service provider that was exempted as of the date of expiry or repeal as if the exemption had never been made.

Exemption de l'application des articles 10 et 11

(4) À la date d'expiration de l'exemption d'une obligation prévue aux articles 10 ou 11 ou de l'abrogation du règlement, l'article en cause s'applique au télécommunicateur pour l'avenir comme si l'exemption n'avait jamais été accordée.

ADMINISTRATION

EXÉCUTION

Designation

33. (1) For the purposes of the administration of this Act, the Minister may designate persons or classes of persons to exercise powers in relation to any matter referred to in the designation.

Désignation

33. (1) Le ministre peut, pour l'exécution de la présente loi, désigner toute personne — individuellement ou au titre de son appartenance à une catégorie — pour exercer des pouvoirs relativement à toute question mentionnée dans la désignation.

Certificate of designation

(2) Designated persons are to receive a certificate attesting to their designation and must, on request, present the certificate to any person appearing to be in charge of any place that they enter.

Certificat

(2) La personne désignée reçoit un certificat attestant sa qualité, qu'elle présente, sur demande, à toute personne apparemment responsable du lieu visité.

Authority to enter

34. (1) A person who is designated to verify compliance with this Act may, for that purpose, enter any place owned by, or under the control of, any telecommunications service provider in which that person has reasonable grounds to believe there is any document, information, transmission apparatus, telecommunications facility or any other thing to which this Act applies.

Powers on entry

(2) The designated person may, for the purpose of verifying compliance with this Act,

(*a*) examine any document, information or thing found in the place and open or cause to be opened any container or other thing;

(*b*) examine or test or cause to be tested any telecommunications facility or transmission apparatus or related equipment found in the place;

(*c*) use, or cause to be used, any computer system at the place to search and examine any information contained in or available to the system;

(*d*) reproduce, or cause to be reproduced, any information in the form of a printout, or other intelligible output, and remove the printout, or other output, for examination or copying; or

(*e*) use, or cause to be used, any copying equipment or means of telecommunication at the place.

Assistance and information

(3) The owner or person in charge of the place and every person who is in the place must give all assistance that is reasonably required to enable the designated person to verify compliance with this Act and must provide any documents, data and information that are reasonably required for that purpose.

Designated person may be accompanied

(4) The designated person, when entering a place referred to in subsection (1), may be accompanied by any person chosen by the designated person.

Warrant for dwelling-house

35. (1) If the place referred to in subsection 34(1) is a dwelling-house, the designated person is not authorized to enter it without the consent of the occupant except under the authority of a warrant issued under subsection (2).

Visite

34. (1) La personne désignée pour vérifier le respect de la présente loi peut, à cette fin, procéder à la visite de tout lieu appartenant à un télécommunicateur — ou placé sous sa responsabilité — où se trouvent, à son avis fondé sur des motifs raisonnables, des installations de télécommunication, des appareils de transmission, des documents, des renseignements ou des objets visés par la présente loi.

Pouvoirs

(2) Elle peut, à cette même fin :

a) examiner les documents, les renseignements ou les objets se trouvant dans le lieu et ouvrir, directement ou indirectement, tout contenant ou autre objet;

b) examiner toute installation de télécommunication ou tout appareil de transmission ou matériel connexe s'y trouvant et lui faire subir, directement ou indirectement, des essais;

c) faire usage, directement ou indirectement, de tout système informatique s'y trouvant pour vérifier les données qu'il contient ou auxquelles il donne accès;

d) reproduire ou faire reproduire toute information sous forme d'imprimé ou toute autre forme intelligible qu'elle peut emporter pour examen ou reproduction;

e) faire usage, directement ou indirectement, du matériel de reproduction et des moyens de télécommunication se trouvant dans le lieu.

Assistance

(3) Le propriétaire ou le responsable du lieu visité, ainsi que quiconque s'y trouve, sont tenus de prêter à la personne désignée toute l'assistance possible pour lui permettre de vérifier le respect de la présente loi et de lui fournir les documents, données et renseignements qu'elle peut valablement exiger.

Personne désignée accompagnée d'un tiers

(4) La personne désignée peut, pour la visite, se faire accompagner de toute personne de son choix.

Mandat pour maison d'habitation

35. (1) Dans le cas d'une maison d'habitation, la personne désignée ne peut toutefois procéder à la visite sans le consentement de l'occupant que si elle est munie du mandat prévu au paragraphe (2).

Authority to issue warrant

(2) On *ex parte* application, a justice of the peace may issue a warrant authorizing a designated person who is named in it to enter a dwelling-house, subject to any conditions that may be specified in the warrant, if the justice is satisfied by information on oath that

(*a*) the dwelling-house is a place referred to in subsection 34(1);

(*b*) entry to the dwelling-house is necessary for the purpose of verifying compliance with this Act; and

(*c*) entry was refused by the occupant or there are reasonable grounds to believe that entry will be refused or that consent to entry cannot be obtained from the occupant.

Délivrance du mandat

(2) Sur demande *ex parte*, le juge de paix peut décerner un mandat autorisant, sous réserve des conditions éventuellement fixées, la personne désignée qui y est nommée à procéder à la visite d'une maison d'habitation s'il est convaincu, sur la foi d'une dénonciation sous serment, que sont réunis les éléments suivants :

a) la maison d'habitation est un lieu visé au paragraphe 34(1);

b) la visite est nécessaire pour vérifier le respect de la présente loi;

c) soit un refus a été opposé à la visite, soit il y a des motifs raisonnables de croire que tel sera le cas ou qu'il est impossible d'obtenir le consentement de l'occupant.

Entry onto private property

36. (1) For the purpose of gaining entry to a place referred to in subsection 34(1), a designated person may enter private property and pass through it, and is not liable for doing so. For greater certainty, no person has a right to object to that use of the property and no warrant is required for entry onto the property unless the property is a dwelling-house.

Droit de passage sur une propriété privée

36. (1) La personne désignée peut, afin d'accéder au lieu visé au paragraphe 34(1), pénétrer dans une propriété privée et y circuler, et ce, sans encourir de poursuites à cet égard; il est entendu que nul ne peut s'y opposer et qu'aucun mandat n'est requis, sauf s'il s'agit d'une maison d'habitation.

Persons accompanying designated persons

(2) A person may, at the designated person's request, accompany the designated person to assist them to gain entry to the place referred to in subsection 34(1) and is not liable for doing so.

Personne accompagnant la personne désignée

(2) Toute personne peut, à la demande de la personne désignée, accompagner celle-ci en vue de l'aider à accéder au lieu, et ce, sans encourir de poursuites à cet égard.

Use of force

37. In executing a warrant to enter a dwelling-house, a designated person must not use force unless they are accompanied by a peace officer and the use of force has been specifically authorized in the warrant.

Usage de la force

37. La personne désignée ne peut recourir à la force dans l'exécution d'un mandat relatif à une maison d'habitation que si celui-ci en autorise expressément l'usage et qu'elle est accompagnée d'un agent de la paix.

False statements or information

38. (1) A person must not knowingly make a false or misleading statement or provide false or misleading information, in connection with any matter under this Act, to a designated person who is carrying out their functions under section 34.

Renseignements faux ou trompeurs

38. (1) Il est interdit à toute personne de faire sciemment une déclaration fausse ou trompeuse ou de communiquer sciemment des renseignements faux ou trompeurs, relativement à toute question visée par la présente loi, à toute personne désignée qui agit dans l'exercice des attributions qui lui sont conférées au titre de l'article 34.

Obstruction

(2) A person must not obstruct or hinder a designated person who is carrying out their functions under section 34.

Entrave

(2) Il est interdit à toute personne d'entraver l'action de toute personne désignée qui agit dans l'exercice des attributions qui lui sont conférées au titre de l'article 34.

ADMINISTRATIVE MONETARY PENALTIES

VIOLATIONS

Violations

39. Every person who contravenes a provision, order, requirement or condition designated under subparagraph 64(1)(*p*)(i) commits a violation and is liable to an administrative monetary penalty not exceeding the prescribed maximum or, if no maximum has been prescribed, to a penalty not exceeding $50,000, in the case of an individual, and $250,000, in any other case.

Designation

40. For the purposes of any of sections 39 and 41 to 53, the Minister may designate persons or classes of persons to exercise powers in relation to any matter referred to in the designation.

NOTICES OF VIOLATION

Issuance and service

41. (1) A designated person may issue a notice of violation and cause it to be served on a person if they believe on reasonable grounds that the person has committed a violation.

Contents of notice

(2) The Minister may establish the form and content of notices of violation, but each notice of violation must

(*a*) set out the name of the person believed to have committed the violation;

(*b*) identify the violation;

(*c*) set out the penalty that the person is liable to pay;

(*d*) inform the person that they may, within 30 days after the day on which the notice is served or within any longer period specified in it, either pay the penalty set out in the notice or make representations with respect to the alleged violation or penalty — including any representations about entering into a compliance agreement — and set out the manner for doing so; and

(*e*) inform the person that, if they fail to pay the penalty or make representations in accordance with the notice, they will be considered to have committed the violation and the penalty will be imposed.

PÉNALITÉS

VIOLATIONS

Violations

39. Toute contravention à un texte désigné en vertu du sous-alinéa 64(1)*p*)(i) constitue une violation passible d'une pénalité ne dépassant pas le maximum réglementaire; à défaut de ce maximum, la pénalité maximale est de 50 000 $, dans le cas des personnes physiques, et de 250 000 $, dans les autres cas.

Désignation

40. Pour l'application de l'un ou l'autre des articles 39 et 41 à 53, le ministre peut désigner toute personne — individuellement ou au titre de son appartenance à une catégorie — pour exercer des pouvoirs relativement à toute question mentionnée dans la désignation.

PROCÈS-VERBAUX

Procès-verbal

41. (1) La personne désignée qui a des motifs raisonnables de croire qu'une violation a été commise peut dresser un procès-verbal qu'elle fait signifier à l'auteur présumé.

Contenu

(2) Le ministre peut déterminer la forme et la teneur des procès-verbaux de violation. Tout procès-verbal mentionne :

a) le nom de l'auteur présumé de la violation;

b) les faits reprochés;

c) le montant de la pénalité à payer;

d) la faculté qu'a l'intéressé soit de payer la pénalité, soit de présenter des observations relativement à la violation ou à la pénalité — y compris en ce qui touche la conclusion d'une transaction —, et ce, dans les trente jours suivant la signification du procès-verbal ou dans le délai plus long précisé dans celui-ci, ainsi que les modalités d'exercice de cette faculté;

e) le fait que le non-exercice de cette faculté vaut aveu de responsabilité et entraîne l'imposition de la pénalité.

Criteria for penalty

(3) The amount of a penalty is, in each case, to be determined taking into account the following matters:

(*a*) that administrative monetary penalties have as their purpose to encourage compliance rather than to punish;

(*b*) the nature and scope of the violation;

(*c*) the person's history of prior violations or convictions — or compliance agreements entered into — under this Act during the five-year period immediately before the violation;

(*d*) the cumulative amount of the penalties that may be imposed for any violation in respect of which section 48 applies;

(*e*) any prescribed criteria; and

(*f*) any other relevant matter.

Détermination du montant de la pénalité

(3) Pour la détermination du montant de la pénalité, il est tenu compte des éléments suivants :

a) le caractère non punitif de la pénalité, laquelle est destinée à encourager l'observation de la présente loi;

b) la nature et la portée de la violation;

c) les antécédents de l'auteur présumé — violation ou condamnation pour infraction à la présente loi ou conclusion de transactions en application de celle-ci — au cours des cinq ans précédant la violation;

d) la totalité des montants des pénalités qui peuvent être imposées en application de l'article 48;

e) tout critère réglementaire;

f) tout autre élément pertinent.

DETERMINATION OF RESPONSIBILITY AND PENALTY

RESPONSABILITÉ ET PÉNALITÉ

Options

42. (1) A person who is served with a notice of violation must, in accordance with the notice, pay the penalty set out in the notice or make representations with respect to the amount of the penalty or the acts or omissions that constitute the alleged violation.

Option

42. (1) La personne à qui est signifié le procès-verbal est tenue, selon les modalités qui sont prévues dans celui-ci, soit de payer le montant de la pénalité, soit de présenter des observations relativement à celui-ci ou aux actes ou omissions en cause.

Deemed violation

(2) A person is deemed to have committed the violation if they either pay the penalty in accordance with the notice of violation or do not pay the penalty and do not make representations in accordance with the notice of violation.

Responsabilité réputée

(2) Vaut déclaration de responsabilité à l'égard de la violation soit le paiement du montant de la pénalité selon les modalités prévues dans le procès-verbal, soit le défaut de paiement si l'intéressé a omis de présenter des observations selon ces modalités.

Making representations

43. (1) The person alleged to have committed a violation may make representations to a designated person other than the one who issued the notice of violation.

Observations

43. (1) L'auteur présumé de la violation peut présenter des observations à toute personne désignée autre que celle qui a dressé le procès-verbal.

Compliance agreement or decision

(2) The designated person to whom the representations are made must either

(*a*) enter into a compliance agreement with the person on behalf of the Minister; or

(*b*) decide on a balance of probabilities whether the person committed the violation and, if so, impose the penalty set out in the

Transaction ou décision

(2) La personne désignée à qui l'auteur présumé de la violation présente des observations :

a) soit conclut avec lui une transaction au nom du ministre;

b) soit détermine, selon la prépondérance des probabilités, sa responsabilité et, le cas échéant, lui impose la pénalité mentionnée au procès-verbal ou une pénalité réduite, ou

notice of violation, a lesser penalty or no penalty, taking into account the matters mentioned in subsection 41(3).

The designated person must cause notice of any decision made under paragraph (*b*) to be issued and served on the person together with written reasons for the decision and notice of the person's right of appeal under subsection 44(1).

Terms of compliance agreements

(3) A compliance agreement

(*a*) may include any terms that the designated person considers appropriate including a requirement that the person alleged to have committed a violation give reasonable security — in a form and an amount that the designated person considers satisfactory — for the person's performance of the agreement; and

(*b*) must provide for payment by the person alleged to have committed a violation to the Receiver General of a specified amount not greater than the penalty set out in the notice of violation if the person does not comply with the agreement.

Agreement ends proceedings

(4) Entry into a compliance agreement ends the violation proceedings and precludes any further violation or offence proceedings in relation to the act or omission in question.

If agreement not complied with

(5) The Minister may issue and serve a notice of default on a person who has entered into a compliance agreement but has not complied with it. On service of the notice, the person is liable to pay without delay the amount provided for in the agreement, failing which, the Minister may realize any security for the person's performance of the agreement.

encore n'impose aucune pénalité, compte tenu des éléments énumérés au paragraphe 41(3).

Elle lui fait signifier avis de la décision motivée prise au titre de l'alinéa *b*) et l'informe par la même occasion de son droit d'interjeter appel au titre du paragraphe 44(1).

Conditions de la transaction

(3) La transaction :

a) peut être assortie des conditions que la personne désignée estime indiquées, notamment la fourniture d'une sûreté suffisante — dont le montant et la nature doivent lui agréer — en garantie de l'exécution de la transaction;

b) doit exiger de l'auteur présumé qu'il verse au receveur général une somme ne pouvant dépasser le montant de la pénalité mentionné au procès-verbal s'il ne se conforme pas aux conditions prévues.

La transaction met fin à la procédure

(4) La conclusion de la transaction met fin à la procédure et fait obstacle à toute autre procédure en violation ou procédure pénale à l'égard de l'acte ou de l'omission en cause.

Avis de défaut d'exécution

(5) Le cas échéant, le ministre peut dresser et signifier à l'intéressé un avis du défaut d'exécution de la transaction, la somme prévue par la transaction devenant exigible, à défaut de quoi le ministre peut réaliser la sûreté.

APPEAL TO MINISTER

Right of appeal

44. (1) A person served with notice of a decision made under paragraph 43(2)(*b*) may, within 30 days after the day on which the notice is served or within any longer period that the Minister allows in accordance with the regulations, appeal the decision to the Minister.

Powers of Minister

(2) On an appeal, the Minister may confirm, set aside or vary the decision of the designated person.

APPEL AUPRÈS DU MINISTRE

Droit d'appel

44. (1) Il peut être interjeté appel auprès du ministre de la décision prise au titre de l'alinéa 43(2)*b*), dans les trente jours suivant la signification de l'avis de la décision ou dans le délai supérieur que le ministre peut accorder en conformité avec les règlements.

Pouvoirs du ministre

(2) Le cas échéant, le ministre confirme, annule ou modifie la décision.

RULES ABOUT VIOLATIONS

Vicarious liability — acts of employees, agents and mandataries

45. A person is liable for a violation that is committed by the person's employee acting in the course of his or her employment or the person's agent or mandatary acting within the scope of his or her authority, whether or not the employee, agent or mandatary who actually committed the violation is identified or proceeded against.

Officers of corporations, etc.

46. An officer, director, agent or mandatary of a person other than an individual that commits a violation is a party to the violation if he or she directed, authorized, assented to, acquiesced in or participated in the commission of the violation and is liable to the administrative monetary penalty provided for that violation whether or not the person that committed the violation has been proceeded against under sections 41 to 43. For greater certainty, an officer or director, or any agent or mandatary who is an individual, is liable only to the penalty provided in respect of an individual.

Defence of due diligence

47. A person is not liable for a violation if they establish that they exercised due diligence to prevent the commission of the violation.

Continuing violation

48. A violation that is committed or continued on more than one day constitutes a separate violation for each day on which it is committed or continued.

Limitation period or prescription

49. Any proceedings in respect of a violation may be instituted at any time within, but not later than, two years after the day on which the subject matter of the proceedings arose.

Violation or offence

50. (1) If it is possible to proceed with any act or omission as a violation and it is also possible to proceed with it as an offence, proceeding in one manner precludes proceeding in the other.

Violation not an offence

(2) For greater certainty, a violation is not an offence.

Non-application of section 126 of *Criminal Code*

(3) Section 126 of the *Criminal Code* does not apply in respect of any obligation or prohibition under this Act whose contravention is a violation under this Act.

RÈGLES PROPRES AUX VIOLATIONS

Responsabilité indirecte — employés et mandataires

45. L'employeur ou le mandant est responsable de la violation commise par son employé ou son mandataire dans le cadre de son emploi ou du mandat, que celui-ci soit ou non connu ou poursuivi.

Cadres des personnes morales

46. En cas de commission par une personne autre qu'une personne physique d'une violation, ceux de ses dirigeants, administrateurs ou mandataires qui l'ont ordonnée ou autorisée, ou qui y ont consenti ou participé, sont considérés comme des coauteurs de la violation et encourent la pénalité prévue, que la personne ayant commis la violation ait été ou non poursuivie au titre des articles 41 à 43. Il est entendu que les dirigeants et administrateurs, ainsi que les mandataires qui sont des personnes physiques, n'encourent que la pénalité prévue pour une personne physique.

Précautions voulues

47. Nul ne peut être tenu responsable d'une violation s'il prouve qu'il a pris toutes les précautions voulues pour prévenir sa commission.

Violation continue

48. Il est compté une violation distincte pour chacun des jours au cours desquels se commet ou se continue la violation.

Prescription

49. Toute procédure en violation se prescrit par deux ans après le fait reproché.

Précision

50. (1) L'acte ou l'omission qualifiable à la fois de violation et d'infraction peut être réprimé soit comme violation, soit comme infraction, la procédure en violation et la poursuite pour infraction s'excluant toutefois mutuellement.

Précision

(2) Il est entendu que les violations ne sont pas des infractions.

Non-application — article 126 du *Code criminel*

(3) L'article 126 du *Code criminel* ne s'applique pas aux obligations ou interdictions prévues par la présente loi dont la contravention constitue une violation aux termes de celle-ci.

Admissibility of documents

51. In any proceeding, in the absence of evidence to the contrary, a document that appears to be a notice issued under subsection 41(1) or 43(2) or (5) or a certificate issued under subsection 53(1) is presumed to be authentic and is proof of its contents.

Admissibilité des documents

51. Dans toute instance, le document qui paraît être un procès-verbal dressé en vertu du paragraphe 41(1), un avis signifié en vertu des paragraphes 43(2) ou (5) ou un certificat de non-paiement établi en vertu du paragraphe 53(1) fait foi, sauf preuve contraire, de son authenticité et de son contenu.

RECOVERY OF PENALTIES AND OTHER AMOUNTS

RECOUVREMENT DES PÉNALITÉS ET AUTRES SOMMES

Debts to Her Majesty

52. (1) A penalty imposed under this Act and an amount referred to in subsection 43(5) each constitute a debt due to Her Majesty in right of Canada and may be recovered in the Federal Court or any other court of competent jurisdiction.

Créance de Sa Majesté

52. (1) Les pénalités et toute somme visée au paragraphe 43(5) constituent des créances de Sa Majesté du chef du Canada, dont le recouvrement peut être poursuivi à ce titre devant la Cour fédérale ou tout autre tribunal compétent.

Limitation period or prescription

(2) No proceedings to recover such a debt may be commenced later than five years after the day on which the debt became payable.

Prescription

(2) Le recouvrement de la créance se prescrit par cinq ans après la date à laquelle elle est devenue exigible.

Proceeds payable to Receiver General

(3) Each such debt is payable to the Receiver General.

Receveur général

(3) Les sommes en cause sont versées au receveur général.

Certificate

53. (1) The Minister may issue a certificate certifying the unpaid amount of any debt referred to in subsection 52(1).

Certificat de non-paiement

53. (1) Le ministre peut établir un certificat de non-paiement pour la partie impayée de toute créance visée au paragraphe 52(1).

Registration in Federal Court

(2) Registration in the Federal Court or in any other court of competent jurisdiction of the certificate has the same effect as a judgment of that court for a debt of the amount specified in the certificate and all related registration costs.

Enregistrement en Cour fédérale

(2) L'enregistrement à la Cour fédérale ou à tout autre tribunal compétent confère au certificat valeur de jugement pour la somme visée et les frais afférents.

OFFENCES AND PUNISHMENT

INFRACTIONS ET PEINES

Misleading statements and information

54. A person must not do any of the following things in performing any obligation under this Act or in any application, declaration or report made under it:

(*a*) knowingly make a false or misleading statement or knowingly provide false or misleading information; or

(*b*) knowingly omit to state a material fact or to provide material information.

Fausses déclarations

54. Il est interdit, dans le cadre de l'exécution d'une obligation prévue par la présente loi ou dans une demande, un rapport ou une déclaration faits sous son régime :

a) de faire sciemment une déclaration fausse ou trompeuse ou de fournir sciemment des renseignements faux ou trompeurs;

b) d'omettre sciemment de mentionner un fait important ou de fournir des renseignements importants.

Offence

55. Every person who wilfully contravenes subsection 6(1) or (2), any of sections 8 to 11, an order made under subsection 14(1) or any

Infraction

55. Quiconque contrevient volontairement aux paragraphes 6(1) ou (2), à l'un ou l'autre des articles 8 à 11, à un arrêté pris en vertu du paragraphe 14(1) ou à tout règlement pris en

regulations made under paragraph 64(1)(*a*) commits an offence and is liable on prosecution by summary conviction

(*a*) in the case of an individual, to a fine not exceeding $100,000; or

(*b*) in any other case, to a fine not exceeding $500,000.

vertu de l'alinéa 64(1)*a*) commet une infraction passible, sur déclaration de culpabilité par procédure sommaire :

a) dans le cas d'une personne physique, d'une amende maximale de 100 000 $;

b) dans les autres cas, d'une amende maximale de 500 000 $.

Offence

56. (1) Every person who contravenes subsection 13(6), section 26, 30 or 54 or a condition referred to in subsection 32(3) is guilty of an offence punishable on summary conviction and liable

(*a*) in the case of an individual, to a fine not exceeding $25,000 for a first offence, or $50,000 for a subsequent offence; or

(*b*) in any other case, to a fine not exceeding $100,000 for a first offence, or $250,000 for a subsequent offence.

Infraction

56. (1) Quiconque contrevient au paragraphe 13(6), aux articles 26, 30 ou 54 ou à toute condition visée au paragraphe 32(3) commet une infraction passible, sur déclaration de culpabilité par procédure sommaire :

a) dans le cas d'une personne physique, d'une amende maximale de 25 000 $ et, en cas de récidive, d'une amende maximale de 50 000 $;

b) dans les autres cas, d'une amende maximale de 100 000 $ et, en cas de récidive, d'une amende maximale de 250 000 $.

Obstruction of designated person

(2) Every person who contravenes subsection 34(3) or 38(1) or (2) is guilty of an offence punishable on summary conviction and liable to a fine not exceeding $15,000.

(2) Quiconque contrevient aux paragraphes 34(3) ou 38(1) ou (2) commet une infraction passible, sur déclaration de culpabilité par procédure sommaire, d'une amende maximale de 15 000 $.

Infraction

Offence

57. Every person who contravenes any provision of this Act or a regulation made under this Act, except in the case of an offence referred to in sections 55 and 56, is guilty of an offence punishable on summary conviction and liable to a fine not exceeding $250,000.

57. Quiconque contrevient à toute disposition de la présente loi ou de ses règlements — sauf s'il s'agit d'une infraction prévue aux articles 55 ou 56 — commet une infraction passible, sur déclaration de culpabilité par procédure sommaire, d'une amende maximale de 250 000 $.

Infraction

Consent of Attorney General of Canada required

58. A prosecution is not to be commenced in respect of an offence referred to in section 55 or subsection 56(1) without the consent of the Attorney General of Canada.

58. La poursuite des infractions prévues à l'article 55 et au paragraphe 56(1) est subordonnée au consentement du procureur général du Canada.

Consentement du procureur général du Canada

Defence of due diligence

59. A person is not to be convicted of an offence under this Act, other than for a contravention of subsection 38(1) or section 54 or an offence referred to in section 55, if they establish that they exercised due diligence to prevent the commission of the offence.

59. Nul ne peut être déclaré coupable d'une infraction à la présente loi, sauf pour une contravention au paragraphe 38(1) ou à l'article 54 ou dans le cas d'une infraction prévue à l'article 55, s'il prouve qu'il a pris toutes les précautions voulues pour prévenir sa perpétration.

Précautions voulues

Officers of corporations, etc.

60. If a person other than an individual commits an offence under this Act, every officer, director, agent or mandatary of the person who directed, authorized, assented to,

60. En cas de perpétration par une personne autre qu'une personne physique d'une infraction à la présente loi, ceux de ses dirigeants, administrateurs ou mandataires qui l'ont ordon-

Cadres des personnes morales

acquiesced in or participated in the commission of the offence is a party to and guilty of the offence and liable on conviction to the punishment provided for the offence whether or not the person that committed the offence has been prosecuted or convicted. For greater certainty, an officer or director, or any agent or mandatary who is an individual, is liable only to the punishment provided in respect of an individual.

née ou autorisée, ou qui y ont consenti ou participé, sont considérés comme des coauteurs de l'infraction et encourent, sur déclaration de culpabilité, la peine prévue, que la personne ayant perpétré l'infraction ait été ou non poursuivie ou déclarée coupable. Il est entendu que les dirigeants et les administrateurs, ainsi que les mandataires qui sont des personnes physiques, n'encourent que la peine prévue pour une personne physique.

Continuing offence

61. If an offence under this Act is committed or continued on more than one day, the person who committed the offence is liable to be convicted for a separate offence for each day on which the offence is committed or continued.

61. Il est compté une infraction distincte pour chacun des jours au cours desquels se commet ou se continue l'infraction à la présente loi.

Infraction continue

Limitation period or prescription

62. Proceedings in respect of an offence under this Act may be instituted at any time within, but not later than, two years after the day on which the subject matter of the proceedings arose.

62. La poursuite de toute infraction à la présente loi se prescrit par deux ans après le fait reproché.

Prescription

Injunctions

63. (1) If a court of competent jurisdiction is satisfied that a contravention of subsection 10(1) or section 11 is being or is likely to be committed, the court may, on application by the Minister, grant an injunction, subject to any conditions that it considers appropriate, ordering any person to cease or refrain from operating the transmission apparatus referred to in subsection 10(1) or to refrain from acquiring, installing or operating the new software referred to in section 11.

63. (1) S'il est convaincu qu'une contravention au paragraphe 10(1) ou à l'article 11 se commet ou est sur le point d'être commise, le tribunal compétent peut, sur demande du ministre, accorder une injonction, assortie des conditions qu'il juge indiquées, interdisant à quiconque, selon le cas, d'exploiter l'appareil de transmission visé au paragraphe 10(1) ou d'acquérir, d'installer ou d'exploiter le nouveau logiciel visé à l'article 11.

Injonctions

Federal Court

(2) For the purposes of subsection (1), the Federal Court is a court of competent jurisdiction.

(2) La Cour fédérale est, pour l'application du paragraphe (1), un tribunal compétent.

Cour fédérale

REGULATIONS

RÈGLEMENTS

Regulations

64. (1) The Governor in Council may make regulations

64. (1) Le gouverneur en conseil peut prendre des règlements :

Règlements

(*a*) respecting the obligations to be performed under subsections 6(1) and (2), including specifying the circumstances in which those obligations do not apply or need not be performed;

a) concernant les obligations prévues aux paragraphes 6(1) et (2), notamment les circonstances où elles ne s'appliquent pas ou celles où il n'est pas nécessaire de les exécuter;

(*b*) respecting the time, manner and form in which the information referred to in paragraph 6(1)(*b*) is to be provided to an authorized person;

b) concernant les modalités de temps et autres afférentes à la fourniture, à la personne autorisée, de l'information visée à l'alinéa 6(1)*b*);

(*c*) respecting the time, manner and form in which an intercepted communication is to be provided to an authorized person;

(*d*) requiring telecommunications service providers to specify the locations where intercepted communications will be provided, respecting the time, manner and form in which the locations are specified and respecting which locations may be so specified;

(*e*) requiring telecommunications service providers to create and keep records with respect to interceptions;

(*f*) respecting the operational requirements referred to in section 7, including matters of time, manner and form in relation to them and the circumstances in which they do not apply or need not be met;

(*g*) for the purposes of paragraph 7(*a*), specifying what is a communication;

(*h*) for the purposes of paragraph 7(*d*)

(i) providing for the minimum number and maximum number of simultaneous interceptions or the manner of determining them,

(ii) prescribing what is to be counted as a single interception,

(iii) respecting the time, manner and form in which a request to increase the number of those interceptions is to be made, the circumstances in which such a request may be made, the time within which the increase is to be made and the duration of the increase, and

(iv) respecting the maximum number of agencies for which a telecommunications service provider is to simultaneously enable interceptions;

(*i*) providing for the global limit referred to in section 12, or the manner of determining it, respecting the circumstances in which it does not apply or need not be met and prescribing what is to be counted as a single interception;

c) concernant les modalités de temps et autres afférentes à la fourniture, à la personne autorisée, de la communication interceptée;

d) exigeant des télécommunicateurs qu'ils précisent les lieux où les communications interceptées seront fournies et concernant les modalités de temps et autres à cet égard et les lieux qui peuvent être ainsi précisés;

e) exigeant des télécommunicateurs la création et la conservation de registres relativement aux interceptions;

f) concernant les exigences opérationnelles prévues à l'article 7, notamment les modalités de temps et autres afférentes et les circonstances où elles ne s'appliquent pas ou celles où il n'est pas nécessaire d'y satisfaire;

g) en ce qui a trait à l'alinéa 7*a*), précisant ce qui constitue une communication;

h) pour l'application de l'alinéa 7*d*) :

(i) prévoyant le nombre minimal et le nombre maximal d'interceptions simultanées ou la façon de les calculer,

(ii) déterminant ce qui constitue une seule interception,

(iii) concernant les modalités de temps et autres visant toute demande d'augmentation du nombre de telles interceptions, les circonstances dans lesquelles elle est faite, le délai pour procéder à l'augmentation et la période visée,

(iv) concernant le nombre maximal d'organismes pour lesquels le télécommunicateur est tenu de permettre des interceptions simultanées;

i) prévoyant la limite globale visée à l'article 12 ou la façon de la calculer et les circonstances où elle ne s'applique pas ou celles où il n'est pas nécessaire de la respecter et déterminant ce qui constitue une seule interception;

j) pour l'application du paragraphe 14(3), établissant les dépenses et les éléments que le ministre doit prendre en considération pour décider d'une indemnité suffisante ou des dépenses nécessaires;

(*j*) for the purposes of subsection 14(3), prescribing expenses and prescribing matters that the Minister is to consider in deciding what amount is reasonable or what prescribed expenses are necessary;

(*k*) for the purposes of subsection 14(5), respecting the provision of notice and assistance;

(*l*) for the purposes of sections 16 and 17, respecting requests made under those sections and the provision of information under those sections, including

(i) specifying the form of that information, the manner of — and time for — providing it and the circumstances under which particular information is to be provided, and

(ii) prescribing any confidentiality or security measures with which the telecommunications service provider must comply;

(*m*) for the purposes of section 18, respecting the creation and retention of records and the dealing with information;

(*n*) for the purposes of section 25, respecting the assistance to be provided in the assessment and testing of telecommunications facilities;

(*o*) for the purposes of section 29, respecting requests for payment and the making of payments;

(*p*) for carrying out sections 39 to 53, including

(i) designating any provision of this Act or of any regulation, or any order or class of orders made under this Act or any requirement or condition of such a provision or order or class of orders — or class of such requirements or conditions — as a provision, order, requirement or condition whose contravention may be proceeded with as a violation,

(ii) prescribing the maximum administrative monetary penalty for a particular violation, which maximum may not exceed $50,000, in the case of an individual, and $250,000, in any other case,

k) pour l'application du paragraphe 14(5), concernant l'avis à donner et l'assistance à prêter;

l) pour l'application des articles 16 et 17, concernant les demandes et la fourniture des renseignements visés à ces articles, notamment :

(i) précisant les modalités de présentation et de temps visant ces renseignements et les circonstances dans lesquelles certains de ceux-ci sont fournis,

(ii) prévoyant les mesures concernant la confidentialité ou la sécurité que le télécommunicateur doit prendre;

m) pour l'application de l'article 18, concernant la création et la conservation des registres et le traitement des renseignements;

n) pour l'application de l'article 25, concernant l'assistance à prêter pour l'évaluation et la mise à l'essai des installations de télécommunication;

o) pour l'application de l'article 29, concernant les demandes de paiement et le versement de ceux-ci;

p) prévoyant les mesures d'application des articles 39 à 53, notamment :

(i) désignant comme texte dont la contravention constitue une violation toute disposition de la présente loi ou de ses règlements, tout arrêté pris en vertu de celle-ci, ou toute catégorie de tels arrêtés, ou toute condition ou exigence prévue — ou catégorie de conditions ou d'exigences prévue — par une telle disposition ou un tel arrêté, ou une telle catégorie d'arrêtés,

(ii) prévoyant le montant maximal — plafonné, dans le cas des personnes physiques, à 50 000 $ et, dans les autres cas, à 250 000 $ — de la pénalité applicable à chaque violation,

(iii) concernant les transactions visées au paragraphe 43(3),

(iii) respecting compliance agreements referred to in subsection 43(3),

(iv) respecting the service of notices referred to in those sections, including the manner of serving them, the proof of their service and the circumstances under which they are deemed to have been served, and

(v) respecting procedure on appeals, which procedure must provide for a reasonable opportunity for the appellant to present written evidence and make representations in writing;

(*q*) prescribing anything that is to be prescribed under this Act; and

(*r*) generally, for carrying out the purposes and provisions of this Act.

(iv) concernant, notamment par l'établissement de présomptions et de règles de preuve, la signification des avis ou des procès-verbaux prévus par ces articles,

(v) concernant la procédure d'appel, qui doit comporter notamment la possibilité pour l'appelant de présenter, par écrit, ses éléments de preuve et ses observations;

q) concernant toute mesure d'ordre réglementaire prévue par la présente loi;

r) d'une façon générale, concernant toute mesure d'application de la présente loi.

Regulations may be limited or vary

(2) Regulations made under subsection (1) may apply generally or to particular classes of telecommunications service providers and may vary by class of telecommunications service provider, by class of telecommunications service provided, by class of telecommunications facility, according to the population of the region in which a telecommunications facility of a given class is located or by the manner in which information is provided.

Catégories

(2) Les règlements peuvent être d'application générale, ou ne viser que telle ou telle catégorie de télécommunicateurs et s'appliquer de manière différente selon la catégorie de télécommunicateurs, la catégorie de services de télécommunication fournis, la catégorie d'installations de télécommunication, la population de la région où est située une installation de télécommunication d'une catégorie donnée ou la façon dont les renseignements sont fournis.

Incorporation by reference

(3) Regulations made under subsection (1) that incorporate documents by reference may incorporate them as amended from time to time.

Incorporation par renvoi

(3) Les règlements qui incorporent des documents par renvoi peuvent les incorporer dans leur version éventuellement modifiée.

COMPENSATION

INDEMNISATION

Consolidated Revenue Fund

65. There is to be paid out of the Consolidated Revenue Fund the sums required to meet the monetary obligations of Her Majesty in right of Canada under subsections 14(3), 21(1) and 29(1).

Paiement sur le Trésor

65. Sont prélevées sur le Trésor les sommes nécessaires pour satisfaire aux obligations pécuniaires de Sa Majesté du chef du Canada aux termes des paragraphes 14(3), 21(1) et 29(1).

Compensation

66. If compensation for the provision of information or specialized telecommunications support is to be paid under section 21 or 29, no such compensation is to be paid under any other Act of Parliament.

Indemnisation

66. Lorsqu'une indemnité peut être payée en vertu des articles 21 ou 29 pour la fourniture de renseignements ou de l'appui spécialisé en télécommunication, aucune indemnité ne peut être payée en vertu d'une autre loi fédérale à ce titre.

REVIEW OF ACT

EXAMEN DE LA LOI

Review

67. Five years after the day on which this section comes into force, a committee of the House of Commons, of the Senate or of both

Examen

67. Cinq ans après la date d'entrée en vigueur du présent article, le comité de la Chambre des communes, du Sénat ou des deux

Houses of Parliament is to be designated or established for the purpose of reviewing this Act.

chambres désigné ou constitué à cette fin entreprend l'examen de l'application de la présente loi.

TRANSITIONAL PROVISIONS

DISPOSITIONS TRANSITOIRES

Delayed application — section 10

68. (1) The application of section 10 with respect to transmission apparatus that a telecommunications service provider begins to operate in the 18-month period beginning on the day on which that section comes into force is suspended for the duration of that period.

68. (1) L'application de l'article 10 à un appareil de transmission que le télécommunicateur commence à exploiter au cours de la période de dix-huit mois commençant à la date d'entrée en vigueur de cet article est suspendue jusqu'à l'expiration de cette période.

Suspension de l'application de l'article 10

Delayed application — section 11

(2) The application of section 11 with respect to transmission apparatus for which a telecommunications service provider installs new software in the 18-month period beginning on the day on which that section comes into force is suspended for the duration of that period.

(2) L'application de l'article 11 à un appareil de transmission pour lequel le télécommunicateur installe un nouveau logiciel au cours de la période de dix-huit mois commençant à la date d'entrée en vigueur de cet article est suspendue jusqu'à l'expiration de cette période.

Suspension de l'application de l'article 11

Presumption — operational requirements

69. (1) A telecommunications service provider that, together with any affiliated or associated telecommunications service provider, has fewer than 100,000 subscribers, without regard to the telecommunications service to which they subscribe, is considered — during the three years after the day on which section 10 or 11 comes into force, as the case may be — to meet any operational requirement in respect of transmission apparatus that the service provider is obligated to meet by virtue of that section if the service provider provides a physical connection point for the transmission apparatus permitting an authorized person to effect an interception.

69. (1) Au cours des trois années suivant la date d'entrée en vigueur des articles 10 ou 11, selon le cas, le télécommunicateur qui, avec les télécommunicateurs qui font partie de son groupe ou avec lesquels il a des liens, compte moins de 100 000 abonnés, tous services de télécommunication confondus, est réputé satisfaire à toute exigence opérationnelle à laquelle il est tenu de satisfaire au titre de l'un ou l'autre de ces articles, s'il fournit un point de raccordement physique à l'appareil de transmission en cause qui permet à toute personne autorisée de procéder à une interception.

Présomption : exigences opérationnelles

Regulations

(2) For the purposes of subsection (1), the Governor in Council may make regulations defining the expression "affiliated or associated telecommunications service provider" and respecting the provision of a physical connection point.

(2) Pour l'application du paragraphe (1), le gouverneur en conseil peut prendre des règlements définissant l'expression « les télécommunicateurs qui font partie de son groupe ou avec lesquels il a des liens » et concernant la fourniture d'un point de raccordement physique.

Règlements

Mandatory reporting — existing service providers

70. Every telecommunications service provider that is providing telecommunications services on the day on which section 30 comes into force must, within six months after that day, submit a report to the Minister in accordance with that section.

70. Le télécommunicateur qui fournit des services de télécommunication à la date d'entrée en vigueur de l'article 30 présente au ministre, dans les six mois suivant cette date, un rapport établi selon les modalités prévues au titre de cet article.

Rapport : télécommunicateurs existants

COORDINATING AMENDMENTS

Bill C-29

71. If Bill C-29, introduced in the 3rd session of the 40th Parliament and entitled the *Safeguarding Canadians' Personal Information Act*, receives royal assent, then, on the first day on which both section 8 of that Act and section 23 of this Act are in force, that section 23 is replaced by the following:

Deemed nature of information

23. Personal information, as defined in subsection 2(1) of the *Personal Information Protection and Electronic Documents Act*, that is provided under subsection 16(1) or 17(1) is deemed, for the purposes of section 7.4 and subsections 9(2.1) to (2.4) of that Act, to be disclosed under subparagraph 7(3)(*c.1*)(i) or (ii), and not under paragraph 7(3)(*i*), of that Act. This section operates despite the other provisions of Part 1 of that Act.

Investigative Powers for the 21st Century Act

72. If a Bill entitled the *Investigative Powers for the 21st Century Act* is introduced in the 3rd session of the 40th Parliament and receives royal assent, then, on the first day on which both section 17 of that Act and subsection 2(1) of this Act are in force, the definition "telecommunications data" in subsection 2(1) of this Act is replaced by the following:

"telecommunications data" *«données de télécommunication»*

"telecommunications data" means data relating to the telecommunications functions of dialling, routing, addressing or signalling 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 or the type of telecommunications service used. It also means any transmission data that may be obtained under subsection 492.2(1) of the *Criminal Code*.

COMING INTO FORCE

Order in council

73. The provisions of this Act, other than sections 71 and 72, come into force on a day or days to be fixed by order of the Governor in Council.

DISPOSITIONS DE COORDINATION

Projet de loi C-29

71. En cas de sanction du projet de loi C-29, déposé au cours de la 3e session de la 40e législature et intitulé *Loi protégeant les renseignements personnels des Canadiens*, dès le premier jour ou l'article 8 de cette loi et l'article 23 de la présente loi sont tous deux en vigueur, cet article 23 est remplacé par ce qui suit :

Dérogation

23. Pour l'application de l'article 7.4 et des paragraphes 9(2.1) à (2.4) de la *Loi sur la protection des renseignements personnels et les documents électroniques*, les renseignements personnels au sens du paragraphe 2(1) de cette loi qui sont fournis au titre des paragraphes 16(1) ou 17(1) sont réputés être communiqués au titre des sous-alinéas 7(3)*c.1*)(i) ou (ii) de cette loi et non de son alinéa 7(3)*i*). Le présent article s'applique malgré les autres dispositions de la partie 1 de la même loi.

Loi sur les pouvoirs d'enquête au 21e siècle

72. Si le projet de loi intitulé *Loi sur les pouvoirs d'enquête au 21e siècle* est déposé au cours de la 3e session de la 40e législature et reçoit la sanction royale, dès le premier jour où l'article 17 de cette loi et le paragraphe 2(1) de la présente loi sont tous deux en vigueur, la définition de «données de télécommunication», au paragraphe 2(1) de la présente loi, est remplacée par ce qui suit :

«données de télécommunication» "telecommunications data"

«données de télécommunication» Données concernant les fonctions de composition, de routage, d'adressage ou de signalisation en matière de télécommunication et indiquant, ou visant à indiquer, l'origine, le type, la direction, la date, l'heure, la durée, le volume, la destination ou la terminaison de la télécommunication produite ou reçue au moyen d'une installation de télécommunication ou le type de service utilisé. Sont également visées les données de transmission obtenues au titre du paragraphe 492.2(1) du *Code criminel*.

ENTRÉE EN VIGUEUR

Décret

73. Les dispositions de la présente loi, à l'exception des articles 71 et 72, entrent en vigueur à la date ou aux dates fixées par décret.

SCHEDULE 1
(Subsections 5(1) and (4) and 14(2))

EXCLUSIONS FROM THE APPLICATION OF THE ACT

PART 1

1. A telecommunications service intended principally for the use of its provider and the provider's household or employees and not by the public.

2. A telecommunications service intended principally for the sale or purchase of goods or services other than telecommunications services to the public.

3. A telecommunications service provided by a financial institution, as defined in section 2 of the *Bank Act*, that enables the business of banking, the trust, loan or insurance business, the business of a cooperative credit society or the business of dealing in securities or other business primarily related to the business of providing financial services.

PART 2

1. Telecommunications service providers whose principal function is operating a registered charity within the meaning of the *Income Tax Act*, other than any service provider in a class listed in Schedule 2, or operating an educational institution other than a post-secondary institution, or operating a hospital, a place of worship, a retirement home or a telecommunications research network, only in respect of telecommunications services that they provide ancillary to their principal function.

2. Telecommunications service providers that are also broadcasting undertakings, as defined in subsection 2(1) of the *Broadcasting Act*, only in respect of broadcasting.

ANNEXE 1
(paragraphes 5(1) et (4) et 14(2))

NON-APPLICATION DE LA LOI

PARTIE 1

1. Services de télécommunication destinés principalement à leur fournisseur, aux membres de sa famille ou à ses employés, et non au public.

2. Services de télécommunication destinés principalement à la vente ou à l'achat par le public de biens ou de services, autres que des services de télécommunication.

3. Services de télécommunication fournis par une institution financière, au sens de l'article 2 de la *Loi sur les banques*, qui permettent à quiconque de se livrer à des activités bancaires ou à des activités fiduciaires, de prêt ou d'assurance, aux activités d'une société coopérative de crédit ou de faire le commerce des valeurs mobilières, ou encore, de toute autre manière, de se livrer à des activités ayant principalement trait à la prestation de services financiers.

PARTIE 2

1. Télécommunicateurs dont l'activité principale consiste à exploiter un organisme de bienfaisance enregistré, au sens de la *Loi de l'impôt sur le revenu* — sauf s'ils appartiennent à l'une ou l'autre des catégories figurant à l'annexe 2 — un établissement d'enseignement autre qu'un établissement d'enseignement postsecondaire, un hôpital, un lieu de culte, une maison de retraite ou un réseau de recherche sur les télécommunications, uniquement pour ce qui est des services de télécommunication qu'ils fournissent de façon accessoire à leur activité principale.

2. Télécommunicateurs qui sont également des entreprises de radiodiffusion au sens du paragraphe 2(1) de la *Loi sur la radiodiffusion*, uniquement pour ce qui est de leur activité de radiodiffusion.

SCHEDULE 2
(Subsections 5(2) to (4) and 14(2) and Schedule 1)
PARTIAL APPLICATION OF THE ACT

PART 1

1. Telecommunications service providers that transmit communications on behalf of other telecommunications service providers, that do not modify particular communications transmitted and that do not authenticate the end users of the telecommunications services of those other service providers, only in respect of the telecommunications services provided to the other service providers.

PART 2

1. Telecommunications service providers whose principal business or function is operating a post-secondary educational institution, a library, a community centre, a restaurant or an establishment that provides lodgings or residential accommodations, such as a hotel, an apartment building or a condominium, only in respect of telecommunications services that they provide ancillary to their principal business or function.

ANNEXE 2
(paragraphes 5(2) à (4) et 14(2) et annexe 1)
APPLICATION PARTIELLE DE LA LOI

PARTIE 1

1. Télécommunicateurs qui transmettent des communications pour le compte d'autres télécommunicateurs et qui ne modifient pas les communications transmises et n'authentifient pas les utilisateurs finaux des services de télécommunication des autres télécommunicateurs, uniquement pour ce qui est des services de télécommunication fournis à ces télécommunicateurs.

PARTIE 2

1. Télécommunicateurs dont l'entreprise ou l'activité principale consiste à exploiter un établissement d'enseignement postsecondaire, une bibliothèque, un centre communautaire, un restaurant, un établissement qui offre des services d'hébergement ou de logement, notamment un hôtel, un immeuble d'habitation ou un immeuble d'habitation en copropriété, uniquement pour ce qui est des services de télécommunication qu'ils fournissent de façon accessoire à leur activité principale.

Published under authority of the Speaker of the House of Commons

Available from:
Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario K1A 0S5
Telephone: 613-941-5995 or 1-800-635-7943
Fax: 613-954-5779 or 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Publié avec l'autorisation du président de la Chambre des communes

Disponible auprès de :
Les Éditions et Services de dépôt
Travaux publics et Services gouvernementaux Canada
Ottawa (Ontario) K1A 0S5
Téléphone : 613-941-5995 ou 1-800-635-7943
Télécopieur : 613-954-5779 ou 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Also available on the Parliament of Canada Web Site at the following address:
Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :
http://www.parl.gc.ca

Available from:
Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario K1A 0S5
Telephone: 613-941-5995 or 1-800-635-7943
Fax: 613-954-5779 or 1-800-565-7757
publications@pwgsc.gc.ca
http://publications.gc.ca

Disponible auprès de :
Les Éditions et Services de dépôt
Travaux publics et Services gouvernementaux Canada
Ottawa (Ontario) K1A 0S5
Téléphone : 613-941-5995 ou 1-800-635-7943
Télécopieur : 613-954-5779 ou 1-800-565-7757
publications@tpsgc.gc.ca
http://publications.gc.ca

Legislative Summary **LS-655E**

BILL C-47: TECHNICAL ASSISTANCE FOR LAW ENFORCEMENT IN THE 21ST CENTURY ACT

Scan

Bill C-47.
on site
Public

Dominique Valiquet
Legal and Legislative Affairs Division

28 July 2009

Library of Parliament
Bibliothèque du Parlement

Parliamentary Information and Research Service

Legislative Summary

LS-655E

BILL C-47: TECHNICAL ASSISTANCE FOR LAW ENFORCEMENT IN THE 21ST CENTURY ACT

Dominique Valiquet
Legal and Legislative Affairs Division

28 July 2009

Library of Parliament
Bibliothèque du Parlement

Parliamentary Information and Research Service

LEGISLATIVE HISTORY OF BILL C-47

HOUSE OF COMMONS		SENATE	
Bill Stage	**Date**	**Bill Stage**	**Date**
First Reading:	18 June 2009	First Reading:	
Second Reading:		Second Reading:	
Committee Report:		Committee Report:	
Report Stage:		Report Stage:	
Third Reading:		Third Reading:	

Royal Assent:

Statutes of Canada

N.B. Any substantive changes in this Legislative Summary that have been made since the preceding issue are indicated in **bold print**.

Legislative history by Michel Bédard

CE DOCUMENT EST AUSSI PUBLIÉ EN FRANÇAIS

CONTENTS

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

BILL C-47: TECHNICAL ASSISTANCE FOR LAW ENFORCEMENT IN THE 21ST CENTURY ACT*

BACKGROUND

A. Purpose of the Bill: Lawful Access

Bill C-47, An Act regulating telecommunications facilities to support investigations (short title: Technical Assistance for Law Enforcement in the 21st Century Act), was introduced in the House of Commons on 18 June 2009, by the Minister of Public Safety (the minister), the Honourable Peter Van Loan.

It deals with very specific aspects of the rules governing lawful access. Lawful access is an investigative technique used by law enforcement agencies(1) and national security agencies that involves intercepting communications(2) and seizing information where authorized by law. Rules relating to lawful access are set out in a number of federal statutes, in particular the *Criminal Code*, the *Canadian Security Intelligence Service Act* and the *National Defence Act*. For greater certainty, the bill provides that law enforcement agencies retain the powers conferred by those Acts.(3)

---

* Notice: For clarity of exposition, the legislative proposals set out in the bill described in this Legislative Summary are stated as if they had already been adopted or were in force. It is important to note, however, that bills may be amended during their consideration by the House of Commons and Senate, and have no force or effect unless and until they are passed by both houses of Parliament, receive Royal Assent, and come into force.

(1) In the interests of conciseness, the term "law enforcement agencies," when used in this text, includes national security agencies, unless otherwise clearly indicated by the context.

(2) Commonly called "wiretapping."

(3) Clause 2(2) of the bill.

This bill complements the current lawful access regime. It addresses the same two issues as the former Bill C-74:[4] technical interception capabilities of telecommunications service providers and requests for subscriber information.

Other aspects of the lawful access regime are addressed in Bill C-46, Investigative Powers for the 21st Century Act, which was introduced on the same day as Bill C-47.

B. Key Measures in the Bill

Bill C-47 addresses a concern expressed by law enforcement agencies, which contend that new technologies, particularly Internet communications, often present obstacles to lawful communications interception. The bill permits the following:

- It compels telecommunications service providers to have the capability to intercept communications made using their networks, regardless of the transmission technology used (clauses 6 to 15).
- It provides law enforcement agencies with access, under an accelerated administrative process without a warrant or court order, to basic information about telecommunications service subscribers. At the same time, the bill provides for certain protection measures (clauses 16 to 23).

C. Basis of the Bill

1. Consultations

Since 1995, the Canadian Association of Chiefs of Police (CACP) has been calling for legislation requiring that all telecommunications service providers have the technical means in place to enable police services to carry out lawful interceptions on their networks.

Following the development of a strategic framework in 2000, representatives of Justice Canada, Industry Canada and the Solicitor General of Canada held public consultations in 2002.[5] After having received more than 300 submissions from police services, industry, civil

---

(4) Bill C-74, An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information, 1st Session, 38th Parliament (died on the *Order Paper*). For more information about this bill, see Dominique Valiquet, *Telecommunications and Lawful Access: I. The Legislative Situation in Canada*, PRB 05-65E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 21 February 2006, http://lpintrabp.parl.gc.ca/LopImages2/prbpubs/bp1000/prb0565-e.asp.

(5) See Justice Canada, Industry Canada, and Solicitor General Canada, *Lawful Access – Consultation Document*, 25 August 2002, http://justice.gc.ca/eng/cons/la-al/consult.html.

rights groups and individuals, Justice Canada released a summary of the results of the consultations in 2003.(6) Throughout the consultations, protection of privacy was one of the central issues in the debate on lawful access. Other significant elements included technical interception standards, costs related to interception capability and the need for new lawful access rules.

The consultations led to the introduction, in November 2005, of Bill C-74, which would have created the Modernization of Investigative Techniques Act, but the bill died on the *Order Paper* before second reading in the House of Commons when a general election was called.

Since then, provincial governments, including British Columbia's, and various Canadian law enforcement agencies have made submissions urging the federal government to adopt lawful access measures. After consulting a broad range of stakeholders, including those from the telecommunications industry, civil liberty groups and victims' rights groups, the federal Minister of Public Safety introduced Bill C-47, which duplicates the fundamental provisions of the former Bill C-74.

2. International Context

Bill C-47 is a key step in the harmonization of legislation at the international level, particularly concerning requirements regarding the interception capabilities of telecommunications service providers. This type of requirement is already found in the legislation of a number of other countries, including the United States, the United Kingdom and Australia.(7)

Canada signed the Council of Europe's *Convention on Cybercrime* in November 2001, as well as its Additional Protocol on hate crime in July 2005. The Convention makes it an offence to commit certain crimes using computer systems and creates legal tools adapted to new technologies, such as orders to produce "subscriber information,"(8) which are similar to the

---

(6) See Nevis Consulting Group (General Editor), *Summary of Submissions to the Lawful Access Consultation*, Department of Justice Canada, 28 April 2003, http://canada.justice.gc.ca/eng/cons/la-al/sum-res/index.html.

(7) For more information on legislation in these countries, see Dominique Valiquet, *Telecommunications and Lawful Access: II. The Legislative Situation in the United States, the United Kingdom and Australia*, PRB 05-66E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 28 February 2006, http://lpintrabp.parl.gc.ca/LopImages2/prbpubs/bp1000/prb0566-e.asp.

(8) Council of Europe, *Convention on Cybercrime*, 23 November 2001, art. 18.

requests for subscriber information set out in Bill C-47. The injunction in the Convention does not specify whether subscriber information can be obtained without a warrant.

Complementary legislation in Bill C-46 includes other provisions, such as those concerning preservation and production orders and the modernization of offences related to computer viruses and hate propaganda, which will enable Canada to ratify the *Convention on Cybercrime* and the Additional Protocol.

DESCRIPTION AND ANALYSIS

A. Interception Capability (Clauses 6 to 15)

1. Current Situation

At present, no Canadian legislation compels all telecommunications service providers to use apparatus capable of intercepting communications. Only licensees that use radio frequencies for wireless voice telephony services have been required, since 1996, to have equipment that permits such interceptions.(9) There is no similar requirement for other telecommunications service providers.

2. Situation Under the Bill

This bill is designed to remedy the absence of standards for the interception capability of telecommunications service providers. It will require all service providers, including, for example, Internet service providers, to possess apparatus enabling law enforcement agencies, once they have obtained a judicial authorization, to intercept communications sent via the service provider. Within six months of the date on which the bill comes into force, telecommunications service providers will have to submit a report to the minister stating their capability to respond to the interception requirements set out in the bill (clauses 30 and 69).

---

(9) This requirement is imposed by Industry Canada when issuing spectrum licences under the *Broadcasting Act*. The rules governing interception are set out in the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications* (revised in November 1995). See Kirsten Embree, "Lawful Access: A Summary of the Federal Government's Recent Proposals – Part I," *Internet and E-Commerce Law in Canada*, Vol. 6, May 2005, p. 18, and Industry Canada, *Spectrum Management and Telecommunications*, "Personal Communications Services," http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf02092.html.

3. Obligations of Telecommunications Service Providers

a. The Capacity to Intercept Telecommunications (Clauses 6(1) and 7(*a*))

The requirement for interception capability relates both to "telecommunications data"[10] and to the actual content of the communication. Telecommunications service providers must use apparatus that enables law enforcement agencies to intercept, for example, subscribers' e-mail and Internet protocol (IP) addresses, the date and time of communications and the types of files transmitted (telecommunications data) and the substance of messages (content-related data).

b. Provision of Requested Information (Clauses 6(1) and 6(5))

Once a law enforcement agency has obtained a judicial authorization, the telecommunications service provider must provide all communications that have been intercepted (clause 6(1)). If possible, the telecommunications service provider must provide the intercepted communication in the form specified by the law enforcement agency (clause 6(5)). The service provider will also be required to give law enforcement agencies, on request, information relating to its facilities and the telecommunications services it offers (clause 6(1)(*b*) and clause 24).

c. Confidentiality (Clause 6(2))

All interception processes must be kept confidential. Telecommunications service providers are thus required to comply with the regulations and to guarantee the security of the contents of the intercepted communication, the telecommunications data and the identity of the individuals and organizations involved.

d. Decryption of Intercepted Communications (Clauses 6(3) and 6(4))

At present, wireless digital communications service providers have an obligation, under their operating licence conditions, to provide law enforcement agencies with decrypted communications. The bill extends that obligation to all technologies. However, if measures taken

(10) See the definition of "telecommunications data" at clause 2(1) of the bill. This means data that identify the origin, destination, date, time, duration, type and size of a telecommunication. This is also sometimes referred to as "traffic data." According to the proposed regulatory policy under the former Bill C-74, a telecommunications service provider lacking the ability to intercept telecommunications data in real time should at least have been capable of intercepting data within one second of intercepting the contents of the communication.

to protect a communication, such as encrypting or encoding, require the telecommunications service provider to develop specific decryption techniques or tools, the telecommunications service provider will not be required to decrypt the intercepted communication.

e. Isolation of the Intercepted Communication (Clause 7(*b*))

A judicial authorization to intercept communications will be made for one or more specific individuals. The telecommunications service provider must therefore be able to separate the communications of the person for whom the authorization is granted from the communications of other users. It must also have the capability to isolate the telecommunications data from the content-related data.

f. Correlation (Clause 7(*c*))

Telecommunications service providers must also have the technical capability to link telecommunications data to the content of an intercepted communication. This will allow the law enforcement agency to associate the offence committed with an IP address, for example.

g. Simultaneous Interceptions (Clause 7(*d*))

Telecommunications service providers are required to allow law enforcement agencies to intercept communications transmitted at the same time by more than one user.[11]

4. Entry Into Force of the Obligations (Clauses 10 and 11)

The bill does not require telecommunications service providers to meet the technical standards for interception capability as soon as the legislation comes into force. Rather, they must do so when updating their systems. Any transmission apparatus acquired or software installed after clauses 10 and 11 come into force must comply with the new standards. However, clause 67 provides that if the acquisition or installation takes place within the 18-month transition period following the coming into force of these two clauses, the application of

(11) Regulations will establish the minimum and maximum numbers of simultaneous interceptions that telecommunications facilities must be able to support (clauses 64(1)(*h*) and (*i*)). The minister may, however, order a service provider to take measures to increase the number of simultaneous interceptions to a number greater than the maximum (clause 14(1)(*b*)).

both clauses will be suspended until the end of the transition period.[12] For example, new software installed nine months after clause 11 comes into force need not comply with the new technical standards until nine months later, at the end of the transition period.

However, the minister will have the power, at the request of the Commissioner of the Royal Canadian Mounted Police (RCMP) or the Director of the Canadian Security Intelligence Service (CSIS), to issue a ministerial order requiring a telecommunications service provider, before upgrading, to acquire communications interception capability that meets the technical standards (clauses 14(1)(*d*) and (*e*)).

B. Requests for Subscriber Information (Clauses 16 to 23)

1. Current Situation

At present, law enforcement agencies need a warrant or court order to obtain personal information about clients from telecommunications service providers.[13]

or consent of TSP

2. Situation Under the Bill

The bill establishes special rules that enable designated people within law enforcement organizations to obtain basic information about a subscriber from a telecommunications service provider, without a warrant or court order.[14] The bill provides for protection measures in relation to such information requests.

---

(12) The former Bill C-74 provided for a 12-month transition period.

(13) See paragraph 7(3)(*c*) of the *Personal Information Protection and Electronic Documents Act*. However, the Ontario Superior Court of Justice ruled that subscribers do not have a reasonable expectation of privacy with respect to basic information held by their Internet service provider (*R.* v. *Wilson*, no. 4191/08, 10 February 2009; see also *R.* v. *Ward*, 2008 CarswellOnt 4728 (Ontario Court of Justice)). The Court found that a subscriber's name and address do not reveal intimate details of his or her lifestyle and personal choices (for more on the notion of "intimate details," see *R.* v. *Plant*, [1993] 3 S.C.R. 281). Previously, the Ontario Court of Justice had ruled otherwise in *R.* v. *Kwok*, [2008] O.J. 2414.

(14) The regulatory policy set out in the former Bill C-74 required designated people to at least provide an identifier associated with the subscriber to prevent "fishing expeditions." For example, to obtain a subscriber's name, the designated person would have to provide an IP address.

3. Request for Information

a. Types of Information That May Be Requested (Clause 16(1))

The information covered by the special rules is strictly limited. The bill lists the information associated with the subscriber's services and equipment that can be obtained without a warrant:

- name;
- address;
- telephone number;
- email address;
- Internet protocol address;
- mobile identification number;
- electronic serial number;
- local service provider identifier;
- international mobile equipment identity number;
- international mobile subscriber identity number; and
- subscriber identity module card number.(15)

Telecommunications service providers are not required to collect information other than the information they already collect in the normal course of business. The bill uses the expression "any information in the service provider's possession or control." As well, they are not required to verify the accuracy of the information they collect.

b. Designated Persons (Clauses 16(3) to 16(5))

Only a designated person may make a request for information under the bill. The person is designated by the Commissioner of the RCMP, the Director of CSIS, the Commissioner of Competition or a chief of police within their respective organizations and must perform duties related to protecting national security or to law enforcement (clause 16(3)).

(15) The definition of "subscriber information" in article 18 of the *Convention on Cybercrime* specifically excludes traffic data.

Each organization may designate a limited number of employees: a minimum of 5% of the agency's employees or, where an organization has 100 or fewer employees, five persons (clause 16(4)).

c. Urgent Situations: Request by a Police Officer (Clause 17)

In an urgent situation that it is reasonably believed may result in serious harm to a person or to property, a police officer – instead of the designated persons – may make a request for information (clause 17(1)).[16] The police officer must, however, inform a designated person in his or her organization, and that person will inform the telecommunications service provider of the request in writing (clauses 17(3) and (4)).

d. Purpose of Request (Clause 16(2))

A request for information may be made only in the course of an investigation by CSIS, the Competition Bureau, the RCMP or another police service, under the applicable legislation. Information obtained in this manner must be used solely for that purpose or for related purposes[17] (clause 19).

e. Confidentiality (Clause 23)

The entire process surrounding the request for information remains confidential. The telecommunications service provider must not inform a subscriber that a designated person has made a request or that it has provided information to the designated person.

4. Protection Measures

The provisions relating to information about subscribers are an attempt to strike a balance between expanding the powers of law enforcement agencies and protecting individuals' privacy. While law enforcement agencies are able to obtain subscriber information without a warrant, the bill does establish certain extrajudicial protection measures.

---

(16) This refers to the same exceptional circumstances as those set out in s. 184.4 of the *Criminal Code*, relating to the interception of communications.

(17) For example, organizations may use the information obtained to lay criminal charges.

Privacy Protection measures:
① Designated Persons must keep records
② Internal audits must be done
③ External audits may be done

a. Records (Clause 18)

It must be possible to trace every request for information. The request must therefore be made in writing (clause 16(1)). Designated persons will also be required to keep a record that contains such details as the reasons for each request and the information obtained.

b. Internal Audits (Clauses 20(1), 20(2), 20(3), 20(7) and 20(8))

The Commissioner of the RCMP, the Director of CSIS, the Commissioner of Competition or a chief of police will be required to take measures to verify, on a regular basis, that the requests made by their organization comply with the provisions in Bill C-47 and its regulations. Among other things, the records and the use made of the information must therefore be examined. Reports concerning the results of the audits must be submitted to the responsible minister and, depending on the law enforcement agency that prepared the report, to the Privacy Commissioner of Canada, the Security Intelligence Review Committee or the provincial public officer responsible for privacy protection.

c. External Audits (Clauses 20(4) to 20(6))

The Privacy Commissioner of Canada (and, in the case of provincial police services, the provincial privacy commissioners, under their respective powers) will have the power to conduct audits to determine whether the RCMP or the Commissioner of Competition is in compliance with the provisions relating to requests for information. The Security Intelligence Review Committee may also undertake audits in respect of CSIS.

C. Enforcement of Bill's Provisions (Clauses 33 to 38)

The minister may designate any person to verify compliance with the provisions of the bill. These individuals may enter any place owned by a telecommunications service provider to examine documents and telecommunications facilities in that place.

D. Violations and Offences (Clauses 39 to 63)

The bill provides for two types of contraventions: violations and offences. It establishes what is essentially a code of penal procedure for violations, which are apparently less serious contraventions. For offences, the summary conviction procedure set out in the *Criminal Code* applies. The bill sets out fines for both types of contraventions. No provision is made for imprisonment.

1. Violations

The Governor in Council will determine, by regulation, which contraventions of the bill constitute a violation (clause 39). The regulations will also establish the maximum fine that may be imposed for each violation. The amount of the fine may not exceed $50,000 in the case of an individual and $250,000 in the case of a corporation (clause 64(1)(*p*)(ii)).

2. Offences

The bill subdivides offences into four categories, based on the amount of the fine that may be imposed:

1. A breach of the obligations relating to capability to intercept, or contravention of a ministerial order, will be liable to maximum fines of $100,000 in the case of an individual and $500,000 in the case of a corporation (clause 55). In addition, if a telecommunications service provider does not have the required interception capability when its system is updated, a court may issue an injunction to prevent the use of transmission apparatus or software (clause 63).
2. Every person who makes a change to a law enforcement agency's interception equipment, fails to submit a report concerning interception capability, makes a false statement or fails to comply with the conditions of a suspension or exemption will be liable to a fine not exceeding $25,000 in the case of an individual ($50,000 for a subsequent offence) or $100,000 in the case of a corporation ($250,000 for a subsequent offence) (clause 56(1)).
3. Failure to cooperate with a designated person verifying compliance with the provisions of the bill or obstructing his or her work will constitute an offence punishable by a maximum fine of $15,000 (clause 56(2)).
4. Every person who contravenes other provisions in the bill will be liable to a maximum fine of $250,000,[18] if the offence in question is not designated by the regulations as a violation (clause 57).

It is important to note that the consent of the Attorney General of Canada is needed before a prosecution may be commenced in respect of the first two categories of offences (clause 58).

(18) For example, provisions relating to requests for subscriber information.

E. Exemptions (Clauses 5, 13, 32 and 68 and Schedules 1 and 2)

The bill will apply to all telecommunications service providers operating a transmission facility in Canada, subject to specified complete and partial exemptions in Schedules 1 and 2. However, the Governor in Council may amend these schedules by regulation to add or delete a class of telecommunications service providers (clause 5(4)). The bill also sets out temporary exemptions for maximum periods of two or three years, depending on the case.

1. Complete Exemptions

a. Private Networks (Clause 5(1), Part 1 of Schedule 1)

The bill contains no provisions that apply to private networks, which means persons who provide telecommunications services primarily to themselves, their household or their employees, and not to the public.

b. Sale or Purchase of Goods and Services (Clause 5(1), Part 1 of Schedule 1)

The bill will not apply to telecommunications service providers that provide telecommunications services intended principally for the sale or purchase of goods or services other than telecommunications services to the public.

c. Specified Institutions (Clause 5(1), Parts 1 and 2 of Schedule 1)

As well, no provision of the bill will apply in the case of:

- financial institutions;
- registered charities;
- educational institutions (except post-secondary institutions);
- hospitals;
- places of worship;
- retirement homes;
- telecommunications research companies; and
- broadcasters.

2. Partial Exemptions

a. Intermediary Telecommunications Service Providers (Clause 5(2), Part 1 of Schedule 2)

Telecommunications service providers that act as intermediaries, that is, that transmit communications on behalf of other telecommunications service providers without modifying communications or authenticating the users, will not be subject to the obligations regarding interception capability when they upgrade their systems or to the obligations in respect of subscriber information. However, they may be made subject to these by order of the minister (clause 14(2)).

b. Specified Institutions (Clause 5(3), Part 2 of Schedule 2)

Apart from the obligation to provide information to law enforcement agencies regarding their telecommunications facilities and services, the bill does not apply to telecommunications service providers whose principle operation is:

- a post-secondary educational institution;
- a library;
- a community centre;
- a restaurant; or
- a hotel or apartment building.

3. Temporary Exemptions

a. Order Suspending Obligations (Clause 13)

The minister may, by order made on the application of a telecommunications service provider, suspend for up to three years, in whole or in part, any obligation relating to interception capability when systems are upgraded. The minister may include any conditions that he or she considers appropriate.

b. Exemption Regulation (Clause 32)

The Governor in Council may, on the recommendation of the minister and the minister of Industry, make a regulation exempting certain categories of telecommunications service providers from the most significant obligations in the bill, including obligations relating to interception capability when systems are upgraded or obligations relating to subscriber information. The exemption may impose conditions and may be valid for a maximum of two years.

c. Telecommunications Service Providers With Fewer Than 100,000 Subscribers (Clause 68)

The bill grants a three-year exemption for service providers with fewer than 100,000 subscribers. During that period, such small service providers will not have to comply with the interception capability standards required when systems are upgraded. However, they must provide a physical connection point permitting law enforcement agencies to intercept communications.

F. Compensation for Telecommunications Service Providers (Clauses 14(3), 21(1) and 29(1))

The bill provides for three situations in which the law enforcement agency must compensate a telecommunications service provider:

- The minister has made an order aimed at, for example, compelling the telecommunications service provider to comply with additional obligations related to interception capability (clause 14(3)).
- The telecommunications service provider has provided subscriber information at the request of the law enforcement agency (clause 21(1)).
- The telecommunications service provider has provided "specialized telecommunications support" to the law enforcement agency (clause 29(1)).

The definition of what constitutes "specialized telecommunications support," as well as the amount of and criteria for compensation will be determined by the regulations.[19]

G. Coming Into Force and Review of Act (Clauses 66 and 71)

The bill will come into force on a day or days set by order of the Governor in Council. Should the bill come into force on more than one day, different provisions would come into force at different times (clause 71).

The bill provides for parliamentary review of the enforcement of its provisions five years after the day on which it comes into force (clause 66).

(19) A recent Supreme Court of Canada ruling shed light on the matter of compensating a telecommunications service provider for costs associated with executing a production order for call data (s. 487.012 of the *Criminal Code*). The Court ruled that various factors should be taken into account, including the breadth of the order being sought, the size and economic viability of the object of the order, and the extent of the order's financial impact on the telecommunications service provider. (*Tele-Mobile Co.* v. *Ontario*, [2008] 1 S.C.R. 305).

C-47 Communications

Setting the Record Straight on Bill C-47

About C-47

- The proposed legislation provides no new powers to intercept communications – police will still require a court order to intercept

- Bill C-47 will bring legislation up to date and into the 21st century to keep pace with new technology and avoid increasing threats to public safety.

- Current legislation does not require telecommunications companies to build in intercept capabilities. Bill C-47 would ensure that over time, companies build these features into their systems.

- Bill C-47 includes some of the safeguards identified by the privacy commissioners to protect privacy. These include such measures as the requirement to track who is requesting information and audits and oversight of how the information is handled.

- A customer name and address is just that, and is considered non-core biographical information. CNA and other subscriber identifying information is not confidential, readily available and also may be publicly available. The subscriber information police will be able to obtain on request definitely does not include such details as a person's chat logs or website visits.

- Obtaining a customer name and address is even less intrusive than running someone's license plate and compared to searches that police need a court order to carry out, such as a wiretap or the search of a home, it is not invasive at all.

- Police require CNA for their daily work. The CNA reporting tool will tell us a lot more about the kinds of situations where police request CNA without a warrant. Examples of when police need to request include:

    - Child sexual exploitation
    - Drugs and organized crime
    - Abduction/missing persons
    - Fraud/financial crime
    - Other

CNA Backgrounder

The RCMP has been working with Public Safety Canada, CSIS, the Department of Justice, and Industry Canada since 1999 to address legislative gaps with respect to law enforcement's ability to lawfully intercept communications, as well as its authority to lawfully obtain subscriber information. The absence of Lawful Access legislation in Canada means that intercepting communications after a lawful authorization has been issued by a judge is too often not possible or not immediately possible. The absence of express legislative authority for police to obtain subscriber information upon request also means police are often forced to obtain a court order for subscriber information, such as a customer name and address (CNA), if a Telecommunications Service Provider (TSP*) will not voluntarily cooperate.

The proposed legislation (Bill C-47) has received second reading and is set to be reviewed by the House of Commons Standing Committee on Public Safety and National Security (the SECU committee). The passage of this legislation will give police the statutory authority to obtain subscriber information from phone companies and ISPs.

Collecting examples and using the on line reporting form

Because of the privacy concerns that the subscriber information provisions attract, it is important that we collect concrete data to clearly demonstrate instances when CNA requests are made and when ISPs do not voluntarily cooperate. The RCMP is asking the law enforcement community, specifically those officers who request CNA information from TSPs as part of their investigations and general duty policing to fill out the online form. This form, which takes a minute or two to fill out will assist us in gathering data to produce statistical evidence in supporting the case for the passage of the subscriber information provisions of the lawful access legislation (Bill C-47).

The RCMP is also looking to CACP to encourage the law enforcement community to gather examples of situations involving investigations and other policing functions where police requested customer name and address information from a telephone company or ISP but were not successful in obtaining the company's cooperation. We are also looking for success stories – examples of voluntary cooperation by TSPs. These examples will help illustrate for Parliament and the public how and why police seek this type of information from these companies and explain why a warrant is not always practical or possible to obtain the information. So these examples are a very important contribution to a better understanding of Bill C-47.

We are also requesting CACP's assistance in injecting these examples in public statements once collected from the RCMP.

- Some Internet Service Providers do not co-operate with law enforcement requests for customer name and address without a warrant, despite the fact that a warrant is not required.

- There is a reluctance to voluntarily co-operate with police for customer name and address requests. In some regions e.g. the Atlantic Region, all ISPs always require warrants.

- Some Internet Service Providers, but not all, recognize they have a social responsibility to cooperate with police with their detection, prevention and early stages of the investigation.

- TSP's lack of co-operation could possibly lead to more victims and more crimes being committed.

- Telecommunications Service Providers (TSPs) includes both Telephone Companies and Internet Service Providers (ISPs)

November 2009

Public Safety Canada / Sécurité publique Canada

DRAFT

Message Event Proposal
LAWFUL ACCESS:
GOVERNMENT OF CANADA INTRODUCES LEGISLATION TO TACKLE CRIME IN TODAY'S HIGH-TECH WORLD

Date: November XX, 2011	**Media Market:**
Time: TBD	
Location: Canadian Parliamentary Press Gallery (TBC) (National Press Theatre) 607-150 Wellington Street Ottawa, Ontario K1P 5A4	**English Media Spokesperson:** - Minister of Public Safety Toews - Minister of Justice Rob Nicholson - RCMP - Federal Ombudsman for Victims of Crime and victims' rights advocates
	French Media Spokesperson: TBD
	Multicultural Media Spokesperson: TBD

THE EVENT

PROACTIVE EVENT OR INVITATION
- Proactive: technical briefing, followed by Ministerial speeches

EVENT
- After former bills C-50, C-51 and C-52 (Lawful Access), have been tabled in Parliament, subject-matter experts will provide media with a technical briefing. Ministers Toews and Nicholson will then hold a press conference to an informed media audience.

GOVERNMENT OF CANADA FUNDING / PARTNER FUNDING:
- N/A

VENUE DESCRIPTION
- National Press Theatre

MEDIA INVITED?
- Yes

MINISTER'S REGIONAL OFFICE CONTACTED (MO to complete)?
- Yes/No

OTHER PARTICIPANTS (MPs, PROVINCIAL REPS, STAKEHOLDERS, ETC)
- Subject matter experts to participate in technical briefing include (TBC):
  - Canadian Association of Chiefs of Police
  - Canadian Police Association
  - Department of Justice counsel
  - RCMP specialists in interception
  - RCMP representatives from the National Child Exploitation Coordination Centre
  - Representative from victims' groups
    - Federal Ombudsman for Victims of Crime (Sue O'Sullivan)

PS-SP-#491512-v9-MEP_-_LA_-_GoC_introduces_legislation_to_tac_2.DOC~~PS-SP-#491512-v9-MEP_-_LA_-_GoC_introduces_legislation_to_tac_1_RCMPinput28Oct2011PS-SP-#491512-v9-MEP_-_LA_-_GoC_introduces_legislation_to_tackle_crime_in_today_s_high-tech_environment.DOC~~

- PS – National Office for Victims (Suzanne Wallace-Capretta, Manager)
- DoJ – Policy Centre for Victim Issues (Corrina Clement, Senior Policy Analyst)
- Ottawa Victim Services (Steve Sullivan, Executive Director, former Federal Ombudsman for Victims of Crime)
- Canadian Resource Centre for Victims of Crime (Heidi Illingworth, Executive Director)

AUDIENCE SIZE AND DESCRIPTION / TARGET AUDIENCES
- Audience size: approx 10-20 national and local media
- Target audiences: victims' groups, law enforcement, business community, privacy advocates, Canadian consumers

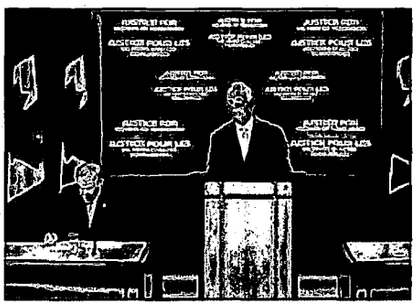
STRATEGIC OBJECTIVES
- To demonstrate the Government's commitment to tackling crime, by providing police with the investigative tools they require to address crime in the 21st century;
- Reassure the Canadian public that this legislation protects their privacy rights by highlighting important safeguards;
- Reassure internet and telecommunications providers, as well as the Canadian public, that costs will be minimized by a gradual phase-in of requirements.

VISUAL MESSAGE(S)

DESIRED PICTURE (STILL)
- Ministers Toews and Nicholson in National Press Theatre

DESIRED PICTURE (VIDEO)
- Minister Toews and Minister Nicholson providing remarks on the new legislation..

ACTUAL SPEAKING BACKDROP
- *National Press Theatre with backdrop words "Tools for law enforcement in the 21st century." (Podium signs not permitted in NPT.)*



LENGTH OF SPEECH
- 3-5 minutes for Minister Toews and 3-5 minutes for Minister Nicholson, followed by 2 minute remarks by the French speaking representative.

TONE
- Positive, authoritative

ATTIRE
- Business

WRITTEN MESSAGE(S)

NEWS RELEASE HEADLINE

Government of Canada introduces new investigative tools for law enforcement

Protecting Canadians by equipping authorities in a high-tech world

DRAFT

DESIRED HEADLINE

- Government of Canada brings in balanced lawful access legislation

DESIRED SOUNDBITE / KEY NEWS RELEASE SOUNDBITE

- "This legislation will enable authorities to keep pace with advances in telecommunications in order to prevent, investigate and prosecute serious crimes, and at the same time put safeguards in place that help to protect the privacy of Canadians."
- "New and evolving technologies make it harder for police to investigate crime, Twenty-first-century technology demands twenty-first-century tools for police to effectively investigate crime, and this legislation provides those tools."

KEY MESSAGES

- Our Government is fulfilling our commitment to take action to protect families and hold criminals accountable.
- Criminals today are using sophisticated technologies to enable their crimes. For instance, members of the Toronto 18 used cell phones and the internet to plan their activities. Just as other countries have updated their laws to reflect this reality, our laws should be updated too.
- This legislation will allow authorities to keep pace with advances in telecommunications technologies in order to prevent, investigate and prosecute serious crimes.
- This legislation will allow authorities to act on judicial authorizations to intercept communications by ensuring that service providers have the technical capability to intercept communications.
- It helps to protect the privacy rights of Canadians while ensuring that the police have the ability to enforce our laws.
- Courts will continue to review and authorize requests to intercept the content of communications, except in exigent circumstances, as is the case today.
- The law would also require that telecommunications service providers supply designated persons with basic subscriber identifying information upon request.
- The basic identifying information that a designated persons would request from a TSP would normally be the name and address, telephone number or e-mail address. It could also, less often, be the Internet protocol address or the name of the local service provider for a subscriber's [telephone?] service or equipment. But none of this basic identifying information will be intimate or highly sensitive information about a person.
- Current legislation allows service providers to provide authorities with basic subscriber information. However, this is carried out informally and voluntarily ~~*on an ad hoc*~~ manner, with some service providers assisting officials, and others not. Furthermore, today there is no system of accountability to ensure the information is ~~accessed~~ obtained properly.
- This legislation will put in place new safeguards that will limit the number of persons designated to request basic subscriber information and will require that each request be documented and regularly reported. None of these safeguards exist today.
- This legislation was the result of years of consultations with a wide range of stakeholders including the telecommunications industry, civil liberties groups, victims' advocates, police associations and provincial and territorial justice and privacy officials.

PROPOSED TWEETS

- Pre-announcement:
- During announcement:
- Post announcement (N/A?)

KEY QUESTIONS AND ANSWERS

Why do we need this ~~to update~~ lawful access legislation?

- *Criminal Code* provisions regarding the interception of communications date back to 1974. Canada's legislation has not kept pace with the rapid evolution of communications and computer technology.
- Because Canada's legislation does not compel telecommunications service providers to develop and maintain intercept capable networks and equipment, the Canadian Security Intelligence Service (CSIS) and police agencies face situations where judicially authorized interceptions cannot be executed. In these instances, investigations and intelligence gathering efforts are sometimes compromised.
- This has allowed criminals and terrorists to benefit from interception "safe havens" and exploit them to continue their activities undetected. This legislation is necessary to eliminate those "safe havens."
- In some cases, authorities have been working with service providers to develop intercept solutions. However, these solutions are often difficult to implement and become obsolete when the providers update their equipment.
- This legislation will put the onus on the companies to incorporate intercept capabilities at the design stage, which is more cost effective than adding the capabilities once the equipment is in use.
- Basic subscriber identifying information is often required at the early stages of investigations and is essential for pursuing investigative leads. The inability to always obtain this information voluntarily ~~in a timely fashion can~~

and efficiently has meant delays or has blocked important investigations -- and that undermines public safety and security.

What is proposed in the new legislation?

- This legislation will obligate telecommunications service providers to have the capability to implement lawful interceptions and to provide basic subscriber identifying information to police, CSIS and Competition Bureau officials upon request.
- It will also introduce much needed consistency and protections for the release of basic subscriber identifying information and will clarify that telecommunications service providers must provide this information to designated police, CSIS and Competition Bureau officials upon request.
- In addition, it would provide law enforcement agencies with new, specialized investigative powers to help them take action against Internet child sexual exploitation, disrupt on-line organized crime activity and prevent terrorism.
- The paperwork application process will also be streamlined when specific court orders or warrants need to be issued in relation to an investigation for which a judge has given a wiretap authorization.

How will this legislation protect Canadians?

- By requiring telecommunications service providers to develop and maintain intercept capable equipment, this legislation will ensure that when authorities are legally authorized to intercept an individual's communications, they won't be unable to do so due to a lack of technical capability on the part of service providers.
- Furthermore, requiring telecommunications service providers to provide basic subscriber identifying information to designated police, CSIS and Competition Bureau officials, will help authorities follow the necessary steps to confirm the identity of individuals who are suspected of committing crimes. The information is also necessary in the conduct of non-criminal police duties such as addressing suicide threats made online.
- Examples of situations where basic subscriber information may be used to help identify an individual include:
  - investigating the sexual exploitation of children;
  - investigating Internet fraud and other online crimes;
  - identifying an incapacitated person carrying only a cell phone;
  - notifying next-of-kin after a car accident;
  - addressing suicide threats over crisis lines; and,
  - returning stolen property to its rightful owner.

RESEARCH NEEDS

- Examples of instances where access to intercepted communications was made difficult
- Examples of instances where access to subscriber information was needed to move ahead on an investigation/arrest

ROLLOUT

COMMUNICATIONS PRODUCTS

- ☒ Media Advisory
- ☒ Speech
- ☒ New Release
- ☒ Backgrounder(s)
- ☒ Media Lines
- ☒ Fact Sheet – "Just the Facts" mythbusting fact sheet to be posted to web page
- ☐ Biographies
- ☐ Talking Points
- ☒ Q&A
- ☐ M.P. Kit
- ☒ Props (Canadian flags)
- ☒ Post-Event Media (Twitter, Facebook)
- ☒ Web Content – Intro + Fact Sheet
- ☐ Photo Release
- ☒ Other (Op-Ed)

OTHER BACKGROUND INFORMATION:

In the past, media has confused these separate, but related pieces of legislation. Former Bills C-50 and C-51 focuses primarily on modernizing legislation to reflect today's high-tech environment and simplifying paperwork processes for warrant applications, while former Bill C-52 is concerned with intercept capability and the provision of basic subscriber information. It will be important to clearly explain each of these components and their implications.

National media coverage on lawful access was minimal between October 1, 2010 just prior to the bills being tabled, and March 26, 2011, when Parliament was dissolved. Coverage focused on financial costs and lack of privacy concerns of the lawful access legislation and was primarily neutral or negative in tone.

Coverage has increased significantly since September 2011, following the tabling of the *Safe Streets and Communities Act,* due to speculation that Lawful Access legislation would be included in the Omnibus Bill. The coverage continued to be neutral or negative in tone and focused on the omission of the lawful access legislation from the *Safe Streets and Communities Act.* Many commentators suggested that the lawful access legislation will be introduced at a later time, while others proclaimed the omission of Lawful Access legislation to be a victory for privacy advocates. During this period, the greatest amount of activity on social media platforms was on Twitter, where users discussed the Act and frequently referenced the absence of the lawful access legislation in the Omnibus Bill.

Coverage since the tabling of the *Safe Streets and Communities Act* has continued to be critical of the lawful access legislation, or "Online Spying", as it has been dubbed by its critics. The primary concern of the critics of lawful access is that it would allow authorities to access private information of any Canadian, at any time, without a warrant. Michael Geist has been a prominent critic of the lawful access legislation for years and has published several articles in the Ottawa Citizen and the Toronto Star. In a November op-ed, he stated that *"Lawful access raises serious privacy and free speech concerns, particularly given the fact that the government has never provided adequate evidence on the need for it, it has never been subject to committee review, and it would cost millions to implement."* Other vocal, proactive and organized critics of the lawful access legislation include OpenMedia.ca & Executive Director Steve Anderson, website The Tyee & blogger Ben Christopher, and Christopher Parsons of the Vancouver Sun, who in a recent column stated, *"Online spying legislation unnecessarily and excessively expands the range of state surveillance capabilities, while removing the judicial constraints that ensure that authorities do not overstep their bounds."* TheMarkNews.com has also worked very closely with OpenMedia.ca to inform readers on the impact of lawful access legislation should it be introduced.

In early October, OpenMedia.ca posted to their website a 14-minute video entitled (un)Lawful Access that is very critical of the lawful access legislation. The video includes commentary from nine experts and journalists, including Michael Geist, David Fewer and Nathalie Des Rosiers.

The CBC, through online and CBC Radio One coverage, has continued to be neutral in their reporting on lawful access. In a late September 2011, CBC Radio One program *Spark*, interviewed two experts (Deputy Chief of the Calgary Police and an internet policy/public Interest advocate) on lawful access and provided balanced coverage of the issue.

Since September, Minister Toews has been particularly vocal in defence of the lawful access legislation. He has expressed his support for the legislation in his column on the mySteinbach.ca website, at a press conference on Oct 3 to launch Canada's cyber security campaign, and in the House of Commons, where he stated *"...outrageous claims... that private communications will be intercepted without a warrant is a complete fabrication...What this will not allow for is access to private communications without a warrant."*

DRAFT

MEDIA PLAN

PLANNING

- ☐ Live Coverage (check if yes)
- ☐ Photographer booked (to distribute photos to media)
- ☐ Readout

STRATEGY

- Insert strategy such as to "maximize coverage (national and regional)," or "target specific media outlets," or "target regional outlets."

PROMOTING THE EVENT

Media Advisory

- Indicate where the advisory will be posted (*some departments include more than one website*)

Contacting Media

- *List media to be contacted by the Minister office (including regional and local media)*

FOLLOW-UP MEDIA (ONE-ON-ONES)

English Media Interviews

- List proposed interviews

French Media Interviews

- List proposed interviews

Multicultural Media Interviews

- List proposed interviews

MEP APPROVED BY:
Name of Minister's Office Staff
Date sent to the Department

Infocapsules de la GRC - *texte définitif*

Date : 1er novembre 2010

Question / Titre
Dépôt de deux projets de loi sur l'« accès légal », *Loi sur les pouvoirs d'enquête au 21e siècle* parrainé par le ministère de la Justice et la *Loi sur les enquêtes visant les communications criminelles et leur prévention* parrainé par Sécurité publique Canada.

Renseignements généraux
L'accès légal est une technique d'enquête importante qu'utilisent les organismes chargés de l'application de la loi et de la sécurité nationale. Dans le contexte de télécommunications au Canada, cet accès comprend l'interception des communications ainsi que la saisie et la perquisition d'information en vertu d'un pouvoir légal conféré par le Code criminel, la *Loi sur le Service canadien du renseignement de sécurité* et d'autres lois du Parlement, dont la *Loi sur la concurrence*.

Ces lois attribuent aux organismes chargés de l'application de la loi et de la sécurité nationale le pouvoir d'intercepter des communications et de saisir et de perquisitionner de l'information conformément aux droits garantis par la Charte canadienne des droits et libertés et surtout le droit à la protection contre les fouilles, les perquisitions et les saisies abusives. L'actualisation la de législation sur l'accès légal figure au programme du gouvernement depuis quelque temps déjà, mais l'adoption des nouvelles dispositions n'a pas encore eu lieu. Donc, le gouvernement dépose les deux projets de loi ci-dessus le 1er novembre. Les principales raisons de la mise à jour de la législation sur l'accès légal sont les suivantes :

- la législation au Canada n'a pas suivi le rythme de l'évolution rapide de la technologie;
- La GRC et d'autres organismes policiers font face à des situations où l'autorisation d'intercepter des communications ne peut être exécutée facilement en raison du manque de capacité technique permettant l'interception sur les réseaux des fournisseurs de services de télécommunications.

Infocapsules

- La GRC appuie l'introduction de tout outil ou processus qui renforce la sécurité du public et hausse l'efficacité de l'application de la loi.
- Le rôle de la GRC n'est pas de commenter les lois à l'étude. Cependant, elle croit que la police a besoin d'outils et de ressources modernes face à l'évolution de la criminalité nationale et transnationale.
- La législation proposée mettrait le Canada sur un pied d'égalité avec d'autres pays qui ont adopté des lois semblables, dont le Royaume-Uni, les États-Unis, l'Australie, l'Allemagne et la Suède.

Préparé par
Jim Spendlove, chef d'équipe, PPS, Services nationaux de communication

Approuvé par :
Elisa Bernstein, officière responsable des Affaires spéciales « I », IOTMP
Helene Van Dyke, conseillère juridique, Services juridiques de la GRC
Patricia Flood, directrice p.i., Relations avec les médias, SNC

P.S. lines from 2010

Public Safety Canada / Sécurité publique Canada

Media Lines

ISSUE: On November 1, 2010, the Government of Canada introduced Bill C-52, the ***Investigating and Preventing Criminal Electronic Communications Act*** to support the interception of communications by the police and the Canadian Security Intelligence Service (CSIS) by requiring intercept capability in telecommunications networks. The law would also provide a procedure for the police, CSIS and the Competition Bureau to obtain ~~with~~ basic subscriber information. This legislation had previously been introduced as the *Technical Assistance for Law Enforcement in the 21st Century Act* (formerly Bill C-4752).

MEDIA LINES:

- The Government of Canada is committed to the safety and security of Canadians and their communities.
- This legislation was drafted to help keep Canadians safe from those who would use new communications technology to pursue criminal or terrorist activities.
- The ***Investigating and Preventing Criminal Electronic Communications Act*** was drafted to ensure that law enforcement and CSIS can keep pace with new communication technologies and are able to execute judicially authorized warrants.
- The legislation drafted did not provide new powers to intercept communications. The warrant processes for the interception of private communications would not change with this Bill.
- The legislation was drafted to provide for a balanced and well-regulated administrative regime for the disclosure of basic subscriber information to the police, CSIS and the Competition Bureau when requested.
- Canada drafted this bill to join many other countries including the United Kingdom, the United States, Australia, Germany and Sweden, which already have similar laws to ensure intercept capability and the sharing of basic subscriber information.

If asked about interception:

- This Government is committed to providing law enforcement and national security agencies with the tools they need to prevent, investigate and prosecute serious crimes including terrorism.

Canada

- While technology has advanced over the past two decades, the technical capability of police to ~~lawfully~~ intercept communications, once they have lawful authority to do so, has not kept pace.

- Courts would continue to review and authorize ~~requests~~applications to intercept communications, as it is the case today.

If asked about subscriber information:

- This legislation was drafted to ensure that the police, CSIS and the Competition Bureau would, upon request, be provided with basic subscriber information.

- Basic subscriber information is often required at the early stages of investigations and is essential for pursuing investigative leads. The inability to obtain this information in a timely fashion can delay or block important investigations and undermine public safety and security.

- This legislation puts in place ~~R~~rigorous safeguards ~~would be put in place~~ to protect subscriber information.

- This drafted legislation was the result of years of consultations with a wide range of stakeholders including the telecommunications industry, civil liberties groups, victims' advocates, police associations and provincial/territorial justice officials.

- The proposed legislation achieved the necessary balance, taking into account the needs of the police, CSIS and the Competition Bureau, and the privacy rights of Canadians.

- It was drafted to help authorities investigate suspected criminals and terrorists who represent a serious threat to the safety and security of Canada.

- This legislation won't let police and intelligence agencies request information about Canadians internet usage (e.g. email content and web browsing) without a warrant.

If asked why subscriber information does not require a warrant:

- Presently, Service providers can voluntarily give ~~requesting~~ basic subscriber information, such as name or address, to police but they can't be compelled to do so without ~~does not require~~ a warrant.

Canada

- The problem is that, while some service providers release basic subscriber information to authorities upon request~~, others fail to provide it in a timely fashion, and~~ others insist on a warrant. However, in many situations, obtaining a warrant for this basic information takes more time or is ~~neither practical nor~~not possible.

- This law was drafted to ensure consistency across the country by compelling telecommunications service providers to disclose basic subscriber information to the police, CSIS and the Competition Bureau when requested.

- As part of our consultations, we heard from authorities about the need for access to basic subscriber information.

- We heard disturbing stories from the National Child Exploitation Co-ordination Centre about cases they could not pursue due to insufficient information. For example:

    - As part of a massive world wide investigation of child pornography, Germany alerted Canadian law enforcement of 200 Internet Protocol addresses associated with online child sexual exploitation.

    - To identify suspects in Canada, ~~T~~the RCMP requested name and address information related to those IP addresses from Internet service providers ~~to identify potential suspects~~. Unfortunately, 47 of those requests were refused.

    ~~o~~As a result ~~T~~there was insufficient information ~~in these cases~~ to obtain warrants. That means these 47 leads had to be reassessed -- for some, further steps might have been taken to continue to pursue the leads but probably for many of them the matter reached a dead-end.~~47 leads reached a dead-end and countless children remain at risk.~~

    ~~o~~

- This proposed legislation was drafted to prevent ~~help to ensure that there are no more~~these kinds of dead-end investigations.

If asked about cost and compensation:

- The legislation would minimize the cost to service providers by:
    - Granting an initial transition period of 18 months for all telecommunications service providers, so as to provide them with time to integrate intercept capability into new equipment and services;
    - Providing reasonable compensation to service providers in instances where the police, CSIS require them to implement intercept capability within the 18 month transition period; and
    - Establishing requirements that allow service providers to select the most cost efficient solution for their particular networks, based on their business practices, rather than imposing the use of specific equipment.

Formatted: Indent: Left: 1", No bullets or numbering

Canada

- This reflects the commitment of the Government to provide a shared response to a shared problem.

Responsive RE compensation:

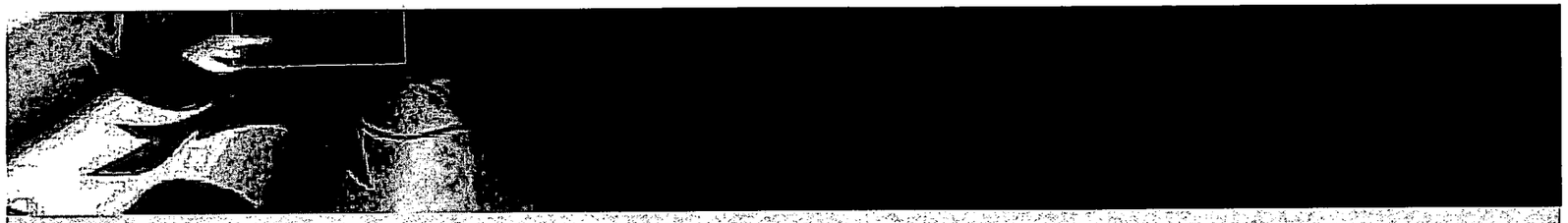
- Service providers are entitled to compensation for the specialized telecommunications support they provide the police and CSIS in implementing interceptions, as well as for providing the police, CSIS and the Competition Bureau with basic subscriber information.

- A fee schedule is currently being developed and will be included in the regulations that will accompany the proposed legislation.

Canada

Every telecommunications service provider must provide a person designated under subsection (3), on his or her written request that includes prescribed identifying information, with any identifying information in the service provider's possession and control respecting the name, address, telephone number and electronic email address of any subscriber to any of the service provider's telecommunications services and the Internet protocol address and local service provider identifier that are associated with the subscriber's service and equipment.

DRAFT – FOR INTERNAL USE



Supporting Lawful Access to Combat Crime and Terrorism

Public Safety and Emergency Preparedness Canada

Sécurité publique et Protection civile Canada

Canada

Context

- Lawful interception of communications is an essential tool for investigating serious offences, organized crime, and national security threats

- The rapidly evolving technological environment is creating obstacles to lawful interception in Canada

- Bill C-XX (formerly Bills C-50, 51 and 52) will equip police, CSIS and the Competition Bureau with the tools they need to ensure criminals and terrorist groups do not exploit technological innovations to hide their illegal activities

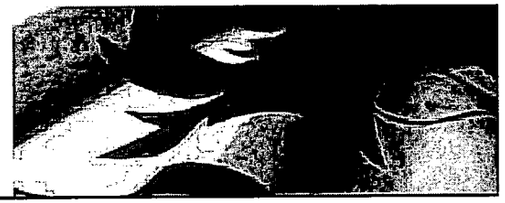
Canada

Proposed Lawful Access Bill

- In October and November 2010, the Ministers of Justice and Public Safety introduced Bills C-50, C-51, and C-52 in the House of Commons
- The Bills died on the Order Paper when Parliament dissolved in March 2011, without having received Second Reading
- The three former bills were combined into the proposed bill, composed of one new statute and various amendments to the *Criminal Code*, the *Competition Act*, and the *Mutual Legal Assistance in Criminal Matters Act*
- The new statute, the *Investigating and Preventing Criminal Electronic Communications Act* (IPCECA) will require telecommunications service providers (TSPs) to:
  - Implement and maintain systems capable of intercepting private communication (intercept-capable systems); and
  - Provide basic subscriber identifying information in a timely fashion to designated police, CSIS and Competition Bureau officials upon request
- The amendments to the three existing statutes include:
  - Streamlining the application process for multiple warrants or orders related to a wiretap investigation;
  - Introducing safeguards for the use of warrantless interceptions conducted under exceptional circumstances (s.184.4 of the *Criminal Code*);
  - Modernizing some investigative powers, including the warrant and production order powers for tracking, number recorders, financial information, and others; and
  - Provisions to enable the ratification of the Council of Europe's *Convention on Cybercrime* and its *Additional Protocol*
- Current thresholds for judicial authorization for interception of communication will not be lowered, and in at least one case will be strengthened
- Consultations took place with various stakeholders to ensure an appropriate balance between investigative needs and the rights of Canadians, while safeguarding the competitiveness of the Canadian industr

Canada

Key Elements: Interception capability



- Telecommunications service providers must develop and maintain a technical capability to enable the lawfully (facilitate judicially) HVD1brized interceptions

- Implementation of the legislation will be flexible and gradual to avoid undue burden on industry:
  - o applies only to newly installed equipment (not retroactive)
  - o transition period (18 months) for Telecommunications service providers HVD3ow time to plan and adjust to requirements
  - o reduced requirements for smaller service providers (<100,000 subscribers) for the first three years
  - o exemptions, as necessary, in defined circumstances
  - o regulatory regime to govern payment for specialized telecommunications support

- The Bill entitles service providers to compensation for specialized telecommunications support related to interception – details to be articulated in the regulations

Canada

Key Elements: Basic Subscriber Information

- Telecommunications service providers must provide this information to designated officials upon request

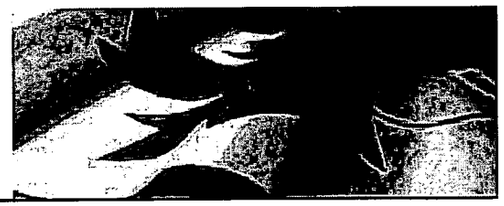
- Only designated police, CSIS and Competition Bureau officials can request basic subscriber information in non-exigent circumstances, which can consist of any of the subscriber's
  - name
  - address
  - phone number
  - email and IP addresses
  - service provider identifier (which TSP they subscribe to)

- Privacy safeguards within the Bill include:
  - subscriber identifiers set out in the Bill
  - request for basic subscriber information is limited to designated personnel, except in exigent circumstances
  - recording of all requests
  - regular internal and periodic external audits
  - all requests must be in the performance of a duty or function of the requesting agency

- TSPs are entitled to compensation for providing basic subscriber information – details to be articulated in the regulations

Canada

Key Elements: Streamlined warrants and public reporting



- Streamlining the process for applications for ~~multiple~~ warrants, or orders related to a wiretap investigation
- Requiring public reporting for interceptions conducted under exceptional circumstances (s.184.4 of the Criminal Code)
- More text needed

Canada

Key Elements: Modernizing investigative powers and ratifying *COC*

DRAFT – FOR INTERNAL USE

- Modernizing some investigative powers, including tracking, number recorders, etc., in the *Criminal Code*, the *Competition Act*, and the *Mutual Legal Assistance in Criminal Matters Act*
- Ratifying the Council of Europe's *Convention on Cybercrime* and its *Additional Protocol*
- More text needed

Canada

Key Elements: Domestic and International Rationale

- Appeals for lawful access have been made by annual resolutions of the Canadian Association of Chiefs of Police, as well as by provincial and federal prosecutors charged with the administration of justice and advocates for crime victims such as the Federal Ombudsman for Victims of Crime

- Many of our international partners have had similar legislation in place for several years

- Canada has been increasingly criticized for being out-of-step with international partners

- The proposed legislation is consistent with that of Australia, New Zealand, United Kingdom, United States and will improve Canada's ability to work with its partners to combat crime and terrorism

- In June 2008, members of the G8 endorsed a declaration that emphasized the need for intercept capability

Canada

Bernard Tremblay - FW: Annonce / Announcement

From: Maillé, Marie Anick<MarieAnick.Maille@ps-sp.gc.ca>
To: Bernard Tremblay <Bernard.Tremblay@rcmp-grc.gc.ca>, Bruce Wallace <bruce.wallace@ic.gc.ca>, "Burton, Meredith" <Meredith.Burton@ps-sp.gc.ca>, "Cintrat, Jean" <Jean.Cintrat@ps-sp.gc.ca>, Douglas Pentland <Douglas.Pentland@bc-cb.gc.ca>, "Durand, Mathieu" <Mathieu.Durand@ps-sp.gc.ca>, "Easson, Grant" <Grant.Easson@ps-sp.gc.ca>, "Haeck, Kimberly" <Kimberly.Haeck@ps-sp.gc.ca>, "Hawrylak, Maciek" <Maciek.Hawrylak@ps-sp.gc.ca>, Helene VanDyke <Helene.VanDyke@rcmp-grc.ca>, Karen Audcent <karen.audcent@justice.gc.ca>, "Kousha, Hasti" <Hasti.Kousha@ps-sp.gc.ca>, "Kwavnick, Andrea" <Andrea.Kwavnick@ps-sp.gc.ca>, Lesley Soper <lsoper@pco-bcp.gc.ca>, LisaFoley <Lisa.Foley@ic.gc.ca>, Maillé, Marie Anick<MarieAnick.Maille@ps-sp.gc.ca>, "Paulson, Erika" <Erika.Paulson@ps-sp.gc.ca>, 'Scott, Marcie" <Marcie.Scott@ps-sp.gc.ca>, "Strasbourg, Christina" <Christina.Strasbourg@ps-sp.gc.ca>, Susan Alter <Susan.Alter@rcmp-grc.ca>, Thomas Dunne <tdunne@pco-bcp.gc.ca>, Trang Dai Nguyen <tnguyen@justice.gc.ca>
Date: 2011-11-16 12:40
Subject: FW: Annonce / Announcement

Merci beaucoup Michèle et bonjour à tous,

I am quite pleased to have joined the National Security Operations team, and thrilled by the opportunity to work with all of you on the lawful access file.

Given the very tight timelines we are facing, my first order of business is to give you a quick "heads-up" that we will be sending you, before the end of today, the following documents for a final fact/substantive check:

- A one page summary of the Bill
- A clause-by-clause analysis of the Bill
- A table identifying the key differences between the bills through time
- A series of one-pagers on important issues
- A "mythbusters" piece
- Qs & As
- A glossary of key definitions / terms

I think this is pretty much it but if I forgot something, it will come in this afternoon's installement.

We will be asking you to provide all your comments, edits and changes before 3 pm this Friday (November 18). We understand this is a small window for your input, but we must finalize and assemble the Ministerial books this Saturday and Sunday -- so we can't stress enough the importance of the Friday deadline. We thank you in advance for your understanding and assistance.

Encore une fois, je remercie en avance pour tout votre travail, et au plaisir de vous rencontrer très prochainement.

Marie Anick Maillé
Senior Policy Advisor | Conseillère principale en politiques
Investigative Technologies and Telecommunications Policy | Technologie d'enquêtes et politiques des télécommunications
National Security Operation Directorate | Direction générale des opérations de sécurité nationale
Public Safety Canada | Sécurité publique Canada
340 avenue Laurier Ave | Ottawa ON K1A 0P9

Telephone | Téléphone: 613.991.3240
E-mail | Courriel: marieanick.maille@ps-sp.gc.ca

From: Kingsley, Michèle
Sent: November 16, 2011 10:38 AM
To: Burton, Meredith; 'Audcent, Karen'; Kousha, Hasti; 'Bernard Tremblay'; 'Douglas.Pentland@bc-cb.gc.ca'; Easson, Grant; Strasbourg, Christina; Haeck, Kimberly; 'Soper, Lesley'; 'Dunne, Thomas'; 'Lisa.Foley@ic.gc.ca'; 'bruce.wallace@ic.gc.ca'; Cintrat, Jean; 'Nguyen, Trang Dai'; Paulson, Erika; 'Helene.VanDyke@rcmp-grc.gc.ca'; 'Susan.Alter@rcmp-grc.gc.ca'; Kwavnick, Andrea; Hawrylak, Maciek; Scott, Marcie; Durand, Mathieu;
Subject: Annonce / Announcement

I am pleased to announce that Marie Anick Maillé has joined our team for a one year assignment as senior policy advisor on the lawful access file. Marie-Anick comes to us from the National Cyber Security Directorate, here at Public Safety Canada, where she managed the cyber engagement and partnerships activities. Before that, Marie-Anick worked for over 5 years at Intergovernmental Affairs - Privy Council Office on complex federal-provincial issues such as national unity, fiscal arrangements, and the management of the federation.

During her tenure with us, Marie Anick will (among other things) coordinate the lawful access interdepartmental working group's process, activities and deliverables. In that regard, I would like to ask you all to keep Marie Anick apprised of all new developments and communications to and for the working group members, and to see her as our single window interface for this same community.

I trust Marie-Anick will be a solid and helpful partner to all of us in this important undertaking. You can reach her at 991-3240 or marieanick.maille@ps-sp.gc.ca.

Thank you, Michèle
****

Je suis heureuse d'annoncer l'arrivée de Marie Anick Maillé pour une affectation d'un an au sein de notre équipe en tant que conseillère principale des politiques sur le dossier de l'accès légal. Elle se joint à nous après une année dans la direction générale sur la cybersécurité nationale, ici à Sécurité publique Canada, où elle était responsable de la mobilisation et des partenariats en matière cybernétique. Elle fut précédemment plus de 5 ans au Secrétariat des Affaires intergouvernementales, au Bureau du Conseil privé, où elle a travaillé sur de nombreuses et complexes problématiques fédérales-provinciales dont l'unité nationale, les arrangements fiscaux et la gestion de la fédération.

Parmi les dossiers dont Marie Anick sera responsable lors de son affectation avec nous, je lui ai demandé de coordonner le processus, les activités et les livrables du groupe de travail interministériel sur l'accès légal. À cet effet, je vous demanderais tous de veiller à informer Marie Anick de tous nouveaux développements ainsi que de toutes communications aux membres du groupe de travail – elle sera notre principal interlocuteur auprès de cette communauté.

Je sais que je peux compter sur Marie-Anick pour nous prêter à nous tous main forte sur le dossier de l'accès légal. Vous pouvez la rejoindre au 991-3240, ou à l'adresse suivante: marieanick.maille@ps-sp.gc.ca.

Merci beaucoup, Michèle

Michèle Kingsley
Director, Investigative Technologies and Telecommunications Policy | Directrice, Technologies d'enquêtes et politiques des télécommunications
National Security Operations | Opérations de la sécurité nationale
Public Safety Canada | Sécurité publique Canada
613.949.3181 / michele.kingsley@ps-sp.gc.ca

Differences between Bills C-74 (2005), C-47 (2009), C-52 (2010), and C-XX (2011)

The substantive differences between the four versions of the lawful access intercept capability bills are detailed below. Note that Bills C-74 and C-XX are omnibus bills which include all legislative aspects of lawful access (led by Public Safety or Justice), while C-47 and C-52 only included the intercept capability and basic subscriber information requirements (led by Public Safety). The DOJ-led aspects of proposed lawful access legislation are not covered in this document.

C-74 (2005)	C-47 (2009)	C-52 (2010)	C-XX (2011)	Section
Have capability to intercept, and provide it when requested by an authorized person	Have capability to intercept	Same	Same	s.6(1)
Ministerial Orders made on opinion of Minister	Ministerial Orders made on opinion of Minister or at RCMP and CSIS request	Same	Same	s.14
No degradation of capabilities and maintaining existing capabilities (s.8 and 9) do not apply to equipment installed by authorities as part of Ministerial Order	No degradation of capabilities and maintaining existing capabilities (s.8 and 9) do not apply to equipment installed by authorities as part of Ministerial Order, but TSP must advise authorities of any problems and provide assistance	Same	Same	s.14
Minister Order prevails over Ministerial Exemptions and any regulations, should there be any inconsistency	Minister Order prevails over any regulations, should there be any inconsistency	Same	Same	s.14
BSI identifiers set out in the regulations	BSI identifiers set out in the legislation	Same	Same	s.16
Designated person is responsible for dealing with information related to BSI requests	Agency that employs the designated persons must retain BSI records and deal with the information that comes from BSI requests	Same	Same	s.18(2)
TSP not required to give access to external auditors for BSI	TSP must give access to external auditors for BSI	Same	Same	s.20(7)
No compensation for BSI	Compensation for BSI	Same	Same	s.21
List of TSP employees providing interception assistance need not be	List of TSP employees providing interception assistance must be updated and disseminated	Same	Same	s.28(2)

updated				
No compensation for interception support	Compensation for interception support	Same	Same	s.29
No mention of any liability for inspector entrance onto private property	Inspector not liable for entry onto private property to get to a place of business, and no one may object to entry	Same	Same	s.36
Criteria for determining the amount of a penalty includes the harm done by the violation and the degree of intention or negligence on the part of the violator	Criteria for determining amount of penalty includes only the nature and scope of the violation	Same	Same	s.41(3)
No regulatory power for: • s.6(2) (location information) • requiring TSPs to keep records on interception • specifying what is a communication • defining the global limit • specifying what notice and assistance must be provided related to agency equipment installed pursuant to a Ministerial Order • what details have to be recorded in BSI records • ops fees	Regulatory power for: • s.6(2) (location information) • requiring TSPs to keep records on interception • specifying what is a communication • defining the global limit • specifying what notice and assistance must be provided related to agency equipment installed pursuant to a Ministerial Order • what details have to be recorded in BSI records • ops fees	Same	Same	s.64(1)
Regulatory power to specify criteria to be taken into account in determining the amount of a proposed penalty	No such power	Same	Same	s.64(1)
No indication of where funds to pay for Ministerial Orders	Funds to pay for Ministerial Orders to come from Consolidated Revenue Fund, which will also pay	Funds to pay for Ministerial Orders to	Same	s.65, 66

are to come from	for ops fees	come from Consolidated Revenue Fund, which will also pay for ops fees; also clarifies that if compensation is paid under ops fees, it will not be paid under other statutes (e.g. CRTC tariffs)		
No review of the Act	5-year Parliamentary review	Same	Same	s.67
Transition period for delayed s.10 and s.11 application is 12 months	Transition period for delayed s.10 and s.11 application is 18 months	Same	Same	s.68
No coordinating amendment with PIPEDA	Same	Coordinating amendment with PIPEDA to clarify that the fact that TSPs must obtain permission from the requesting agency before notifying a subscriber that their information had been provided to the agency	Same	Old s.71
No coordinating amendment to include new definition of "transmission data" from other legislation (this was an omnibus bill so it was included already)	Coordinating amendment to include new definition of "transmission data" from C-46	Same	No coordinating amendment to include new definition of "transmission data" from other legislation (this was an omnibus bill so it was included already)	Clause 45 (old s.72)
Schedule 1 Part 1 exempts households	Schedule 1 Part 1 exempts households, online retailers, and banks	Same	Same	Sch. 1 Part 1

Notes

- The relocation of s.30 in C-74 to s. 70 in C-52 has not been classified as a change, since all it does is changes the placement.

- Small differences in the AMPs regime, notably where mention of certain sections as contraventions were added or removed, have not been recorded.
- Minor changes in regulatory powers in this document have not been recorded.

Drafted: NSOD/Hawrylak
Date 15 November 2011

OVERVIEW OF BILL C-XX
MODERNIZING CRIMINAL INVESTIGATION POWERS ACT

The *Modernizing Criminal Investigation Powers Act* is a comprehensive bill that contains one new statute – the *Investigating and Preventing Criminal Electronic Communications Act* (IPCECA) – and amendments to the *Criminal Code*, the *Competition Act*, and the *Mutual Legal Assistance in Criminal Matters Act*. This Bill is a response to the growing complexity of telecommunications technologies that underpin modern life, which have outstripped the ability of authorities to keep pace and are exploited by criminals to hide their illegal activities. Earlier iterations of this Bill were introduced in 2005, 2009, and most recently in 2010 as Bills C-50, C-51 and C-52. The Bill contains six principal components.

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

Basic subscriber information. Bill C-XX provides the police, CSIS and the Competition Bureau consistent and reliable access to basic subscriber information, which is often required at the early stages of investigations or to fulfill general policing duties. This information is currently provided without a warrant under existing legislation, on a voluntary basis, which results in inconsistent access and delay. Authorities may request any or all of the subscriber's name, address, telephone number, e-mail address, Internet Protocol address, and local service provider identifier. The Bill introduces strict controls and protections for the release of basic subscriber information, including record-keeping and audits, none of which exist today. Basic subscriber information is the second component of the new IPCECA statute.

Streamlined court order application process. The Bill reduces delays and inconsistencies inherent in the judicial authorization process for multiple investigative techniques under the *Criminal Code*. Currently, police have to apply for different warrants – interception, tracking, dialed number recorder, etc. – separately. Bill C-XX will allow police to apply to a single judge for all the warrants relating to the same investigation simultaneously (ensuring that one judge has the full picture of the investigation), harmonize the timeframes, and receive automatic sealing to prevent disclosure to the person targeted by the investigation.

New safeguards for warrantless interceptions. Bill C-XX improves the public accountability of the interception regime by introducing annual public reporting of interceptions conducted lawfully, but without judicial authorization, in exceptional circumstances. The Bill also includes provisions to notify individuals whose communications have been intercepted under these same circumstances. These provisions would match those already included in the *Criminal Code* for interceptions in normal circumstances, which must receive judicial authorization.

Modernizing some investigative powers. The Bill amends substantive offences and procedural powers of the *Criminal Code* to better address cybercrime and update the *Code* to enable it to respond to today's telecommunications reality. New classifications will be established for certain production orders to reflect modern technologies, including for accessing transmission data. Finally, a new data preservation power will allow police to require TSPs to preserve computer data, for specified periods not exceeding 90 days. In such cases, however, the police must return to the TSP with judicial authorization in order to access the preserved data.

Ratifying the *Convention on Cybercrime*. Canada signed the Council of Europe's *Convention on Cybercrime* – the only existing international treaty on cybercrime – and its *Additional Protocol* criminalizing online hate activities in 2001 and 2005, respectively, but has yet to ratify it. The amendments proposed in this Bill will allow Canada to ratify this important Convention and improve international cooperation on cybercrime. Ratification will also allow Canada to meet its G8 commitments on the matter.

These tools are essential for the investigation and prosecution of serious offences such as child pornography, drug trafficking and terrorism. The Bill maintains or in some instances strengthens current thresholds for judicial authorization, and strikes the right balance between providing authorities with the tools they need to fight crime in the 21st century, and protecting the fundamental rights of Canadians.

DRAFT – FOR INTERNAL USE

Public Safety Canada / Sécurité publique Canada

BUILDING A SAFE AND RESILIENT CANADA

The Modernizing Criminal Investigation Powers Act

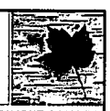
Briefing

November 16, 2011 11:21am

Canada

DRAFT – FOR INTERNAL USE

Context



BUILDING A SAFE AND RESILIENT CANADA

- The rapidly growing number of telecommunications service providers (TSPs) and the diffusion of technology into every aspect of modern life has a significant impact on criminal law
- Legal frameworks and investigative practices are challenged to keep pace with this evolution
- Lawful interception of communications is an essential tool for investigating serious offences, organized crime, and national security threats
- Bill C-XX (formerly Bills C-50, 51 and 52) will equip police, CSIS and the Competition Bureau with the tools they need to ensure criminals and terrorist groups do not exploit technological innovations to hide their illegal activities

Public Safety Canada / Sécurité publique Canada

1

DRAFT – FOR INTERNAL USE

Domestic and International Rationale

BUILDING A SAFE AND RESILIENT CANADA

- Appeals for lawful access legislation and updates to existing laws have been made by annual resolutions of the Canadian Association of Chiefs of Police, as well as by provincial and federal prosecutors charged with the administration of justice and advocates for crime victims such as the Federal Ombudsman for Victims of Crime
- Many of our international partners have had similar legislation in place for several years
- Canada has been increasingly criticized by international partners for being out-of-step with international partners
- The proposed legislation is consistent with that of Australia, New Zealand, United Kingdom, United States and will improve Canada's ability to work with its partners to combat crime and terrorism
- In June 2008, members of the G8 endorsed a declaration that emphasized the need for intercept capability

DRAFT – FOR INTERNAL USE

Proposed Lawful Access Bill

BUILDING A SAFE AND RESILIENT CANADA

- In October and November 2010, the Ministers of Justice and Public Safety introduced Bills C-50, C-51, and C-52 in the House of Commons
- The Bills died on the Order Paper when Parliament dissolved in March 2011, without having received Second Reading
- The three former bills were combined into the proposed omnibus bill, composed of one new statute and various amendments to the *Criminal Code*, the *Competition Act*, and the *Mutual Legal Assistance in Criminal Matters Act*
- Consultations took place with various stakeholders to help ensure an appropriate balance between investigative needs and the rights of Canadians, while safeguarding the competitiveness of the Canadian industry – however, privacy advocates continue to oppose the bill

DRAFT – FOR INTERNAL USE

Basic Elements

BUILDING A SAFE AND RESILIENT CANADA

- The new statute, the *Investigating and Preventing Criminal Electronic Communications Act* (IPCECA) will require TSPs to:
  1. implement and maintain systems capable of lawfully intercepting private communications; and
  2. provide basic subscriber information in a timely fashion to designated police, CSIS and Competition Bureau officials upon request

- The amendments to the *Criminal Code*, the *Competition Act*, and the *Mutual Legal Assistance in Criminal Matters Act* include:
  3. streamlining the application process for court orders related to an interception investigation;
  4. introducing safeguards for ~~the use of warrantless~~ interceptions conducted in exceptional circumstances (s.184.4 of the *Criminal Code*);
  5. modernizing some investigative powers, including ~~the warrant and~~ production order ~~powers~~ for tracking and number recorders; and
  6. amendments to enable the ratification of the Council of Europe's *Convention on Cybercrime* and its *Additional Protocol*

- Current thresholds for judicial authorization will be maintained or strengthened

Public Safety Canada / Sécurité publique Canada

4

DRAFT – FOR INTERNAL USE

1. Interception capability

BUILDING A SAFE AND RESILIENT CANADA

- Telecommunications service providers must develop and maintain a technical capability to enable lawfully authorized interceptions

- Implementation of the legislation will be flexible and gradual to avoid undue burden on industry:
  - applies only to newly installed equipment (not retroactive)
  - transition period (18 months) to allow TSPs time to plan and adjust to requirements
  - reduced requirements for smaller service providers (<100,000 subscribers) for the first three years
  - exemptions, as necessary, in defined circumstances

- The Bill entitles service providers to compensation for specialized telecommunications support related to interception – details to be articulated in the regulations

Public Safety Canada / Sécurité publique Canada

5

Review today for PS (call Stu

DRAFT – FOR INTERNAL USE

2. Basic S…

BUILDING A SAFE AND RESILIENT CANADA

- Telecommunications service providers must provide basic subscriber information to designated officials upon request
- Only designated police, CSIS and Competition Bureau officials can request basic subscriber information in non-exigent circumstances, which can consist of any of the subscriber's
  - name
  - address
  - phone number
  - email address
  - IP address
  - service provider identifier (which
- Designated officials must provide a p… (e.g. name) to obtain basic subscribe…
- TSPs are entitled to compensation fo… details to be articulated in the regulations

Stats
– Multiple
↳ refusal

DRAFT – FOR INTERNAL USE

2. Basic Subscriber Information Safeguards

BUILDING A SAFE AND RESILIENT CANADA

- Privacy safeguards for basic subscriber information include:
  - request for basic subscriber information is limited to designated personnel (except in exigent circumstances) – maximum 5% of the employees of an organization
  - information to be provided to the requesting official is limited to the identifiers set out in the Bill
  - Record-keeping requirements
  - regular internal audits, and external audits by appropriate third parties (such as the federal Privacy Commissioner in the case of the RCMP)
  - all requests must be in the performance of a duty or function of the requesting agency

DRAFT – FOR INTERNAL USE

2. Basic Subscriber Information

BUILDING A SAFE AND RESILIENT CANADA

- Telecommunications service providers must provide basic subscriber information to designated officials upon request
- Only designated police, CSIS and Competition Bureau officials can request basic subscriber information in non-exigent circumstances, which can consist of any of the subscriber's
  - name
  - address
  - phone number
  - email address
  - IP address
  - service provider identifier (which TSP they subscribe to)
- Designated officials must provide a piece of prescribed identifying information (e.g. name) to obtain basic subscriber information
- TSPs are entitled to compensation for providing basic subscriber information – details to be articulated in the regulations

Public Safety Canada Sécurité publique Canada

6

DRAFT – FOR INTERNAL USE

2. Basic Subscriber Information Safeguards

BUILDING A SAFE AND RESILIENT CANADA

- Privacy safeguards for basic subscriber information include:
  - request for basic subscriber information is limited to designated personnel (except in exigent circumstances) – maximum 5% of the employees of an organization
  - information to be provided to the requesting official is limited to the identifiers set out in the Bill
  - Record-keeping requirements
  - regular internal audits, and external audits by appropriate third parties (such as the federal Privacy Commissioner in the case of the RCMP)
  - all requests must be in the performance of a duty or function of the requesting agency

Public Safety Canada Sécurité publique Canada

7

DRAFT – FOR INTERNAL USE

3. & 4. Streamlined process for related warrants and new safeguards

BUILDING A SAFE AND RESILIENT CANADA

- Provide a single process for obtaining court orders relating to an investigation for which an interception authorization was obtained
  - reduces delay by going to one judge instead of several
  - introduces a consistent authorization timeframe for all investigative techniques
  - increases safety by automatically sealing all warrants related to the interception investigation from disclosure
- Add safeguards of reporting and notification to section 184.4 (interception of private communications in exceptional circumstances) of the *Criminal Code*
  - Interceptions made pursuant to s.184.4 of the *Code* must be reported annually
  - A person whose private communications were intercepted by virtue of s.184.4 of the *Code* must be notified within specified timelines

Public Safety Canada Sécurité publique Canada

8

DRAFT – FOR INTERNAL USE

5. & 6. Modernizing offences and ratifying Convention on Cybercrime

BUILDING A SAFE AND RESILIENT CANADA

- Amends substantive offences and procedural powers of the *Criminal Code* to better address cybercrime and crimes committed using new technology
  - new power requires TSP to preserve data for specified period
    - no disclosure of information – merely a "do-not-delete" requirement, and officer must seek warrant to release actual content
  - includes production orders for tracking data, transmission and general data, financial data and tracing communications (partial disclosure)
  - introduces new or updated warrant powers
    - dialled number recorder (for phones) updated to include computer transmission data (bill also proposes to allow this without a warrant in exceptional circumstances)
    - new tracking warrant raises judicial threshold for authorization if the tracking device is on the person (e.g. cell phone)
- All amendments maintain or strengthen oversight thresholds, and create proper balance between investigative need and privacy protection
- Permits ratification of the Council of Europe *Convention on Cybercrime* and the *Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*

Public Safety Canada Sécurité publique Canada

9

Hot Issues:
Myths About Lawful Access Legislation

Myth: Compelling telecommunication service providers to provide basic subscriber information to authorities upon request, and to police in emergencies, will automatically give authorities access to the contents of an individual's communications.

Fact: Access to the actual content of communications, or tracking of an individual or a telecommunications device, will continue to require judicial authorization, except in exigent circumstances, as per current legislation governing interception.

- Providing basic subscriber information to authorities refers to just that: the provision of information limited to a customer's name, address, telephone number, email address, Internet Protocol address at a given date and time,
- Basic subscriber information only reveals identification information about a person, and only at a specific point in time.
- Having access to this basic information does not physically or legally allow police, CSIS and the Competition Bureau to have access to information pertaining to the content of emails, websites an individual visited, phone calls either made or received, or tracking an individual's activities,

Myth: "Warrantless access" to basic subscriber information lacks oversight, and will give police and government unregulated access to our personal information.

Fact: Federal legislation *already allows* service providers to release basic subscriber information to police, CSIS and the Competition Bureau without a warrant.

Lawful Access legislation will put into a place a number of checks and balances concerning the collection and use of this information which do not exist today, specifically:

- Limiting the number of officials who can request basic subscriber information to a maximum of five people per organization, or 5% of the organization's workforce (whichever is greater);
- Putting procedures in place for mandatory record keeping by authorities of all requests for basic subscriber information;
- that basic subscriber information may only be requested in order to perform a duty or function of the agency in which a designated officials works;
-

1

- Mandating regular internal audits be conducted by the heads of respective agencies, and requiring that reports on the findings of these audits be provided to the responsible Minister and to the responsible external review bodies;
-
- Requiring that telecommunications service providers comply with the confidentiality and security measures included in the regulations.

Myth: Basic subscriber information provisions go way beyond accessing "phone book information".

Fact: The basic subscriber information contained within the legislation is the modern day equivalent of information that is accessed from the phone book. These identifiers are often searchable online, shared between individuals,

- Name, address, and telephone number are available on publicly available websites or in the actual phone book.
- People provide their names, addresses and home phone and cell phone numbers on a daily basis to apply for credit cards, enter into contests, and to socially connect.
- Email addresses are designed to be shared, and are given out by Canadians so that they may connect with other people.
- Every time someone uses the internet, their IP address is shared with the website that they are accessing, and is often visible in chat rooms or other public spaces online.
- In general, these identifiers are voluntarily and repeatedly released by individuals for a large number of purposes, which reveals a high expectation that this information will be publicly known.

Myth: Lawful Access legislation is adding new "surveillance" powers, and will inevitably result in an increase in the tracking of Canadians and/or the interception of their communications.

- Production orders related to transmission data and tracing of specified communications, which were previously obtained using general warrants, will be

reclassified under new categories. These orders will adopt the judicial authorization threshold that is already employed by existing specific production order powers

- Bill C-XX will also rectify a gap in powers related to the transmission data recorder (a machine that records the basic transmission information about a communication, rather than its content), by allowing police to use such a device in exceptional circumstances without a warrant. This simply brings transmission data recorder powers into line with other similar techniques with respect to the ability to use them without a warrant in exceptional circumstances.

- In addition, the new statute created by the Bill, IPCECA, will require that telecommunication service providers be intercept capable so that authorities can intercept communications in an efficient manner when they are legally authorized to do so. No new interception or tracking ("surveillance") powers are included in IPCECA, and the interception and tracking of individuals continues to require lawful authorization.

-

Myth: Lawful Access legislation will the privacy rights of Canadians.

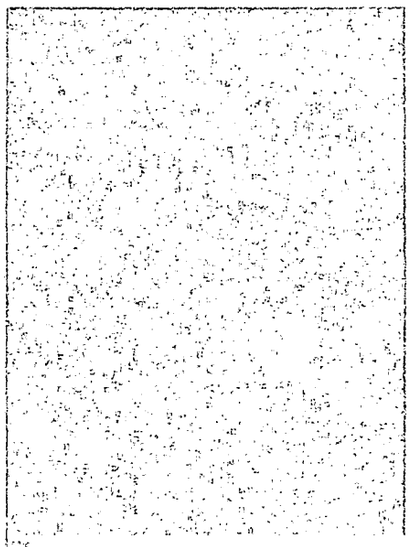
Fact: Lawful Access legislation will put into place a number of safeguards that currently do not exist regarding access to basic subscriber information (as discussed above), and will also maintain or strengthen legal thresholds for provisions with the *Criminal Code* and related statutes to ensure a proper balance between investigative needs in the 21st century and privacy protection.

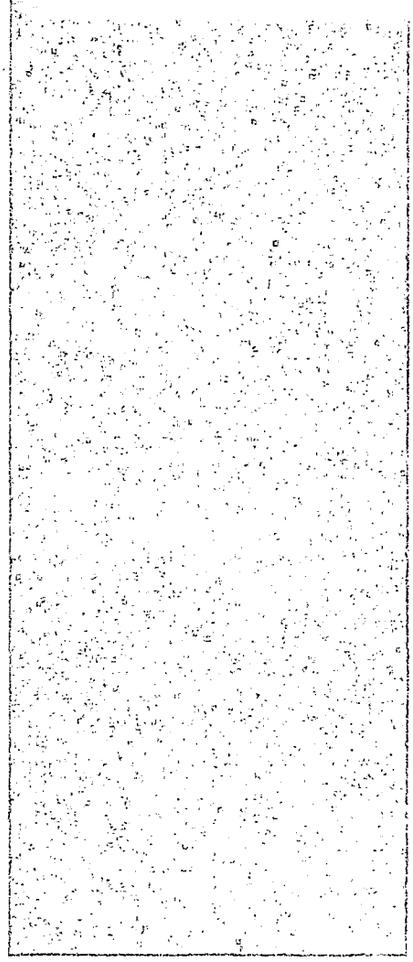
- For example, it has been recognized that authorities may at times be required to intercept communications without a warrant in exigent circumstances, which they are authorized to do under the *Criminal Code*. Proposed amendments to the *Criminal Code* will further clarify expectations respecting this section by putting in writing certain safeguards, such as annual reporting and notification to the individual whose communications have been intercepted.

Myth: Lawful Access legislation will *require* telecommunication service providers to maintain a database of information about their customers, and authorities will have access to this database upon request.

Fact: Lawful Access legislation does not compel service providers to keep information about all customers at all times. The Bill will allow police to compel a TSP to preserve historical computer data of a specific subscriber until such time as the police can get a warrant to access it. Authorities can only request the preservation of data already in control of the TSP.

- This data must be related to a specific individual(s) where authorities believe that such data will assist in a specific investigation.





- Ultimately, in order to receive the contents of the communications being held under a preservation order or demand, the judicially authorized production order or a warrant. Without it, TSPs are not obligated to continue to preserve any information.

Myth: Lawful Access legislation will be expensive for industry, passing along costs to consumers.

Fact: Lawful Access legislation contains a number of mechanisms that would minimize the cost to service providers.

- The intercept capability requirements within the new legislation, IPCECA, are forward-looking,

  The legislation was designed this way as it was recognized that it is more cost-effective to incorporate capability at the design stage than it is to include it in equipment already in use. In addition, the legislation:

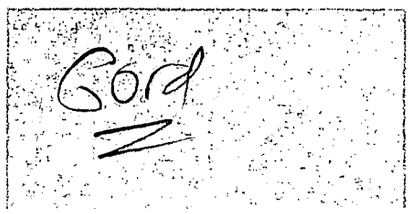
- Grants an initial transition period of 18 months for all telecommunications service providers, during which time the operational requirements would be suspended. This would allow TSPs time to test and integrate intercept capability into new equipment and services;

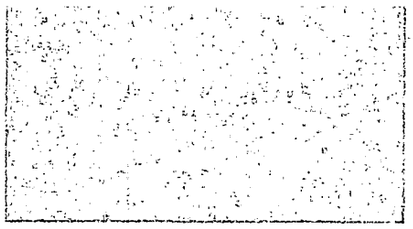
- Provides reasonable compensation to service providers in instances where the police or CSIS require them to implement intercept capability within the 18 month transition period;

- Allows service providers to select the most cost efficient solution for their particular networks, based on their business practices, rather than imposing the use of specific equipment; and,

- Provides compensation to service providers for the specialized telecommunications support they provide the RCMP and CSIS in implementing interceptions, as well as

for providing the police, CSIS and the Competition Bureau with basic subscriber information.





RCMP Media Lines – *Draft 5*

Date: November 24, 2011

Issue/Title
November 29 tabling of "lawful access" legislation, formerly Bills C-50, C-51 and C-52, which have been amalgamated into one Bill: C-XX

Background
Lawful access is an important investigative technique used by law enforcement and national security agencies. In the context of telecommunications in Canada, it consists of the interception of communications and search and seizure of information carried out under legal authority as per the *Criminal Code (CC), the Canadian Security Intelligence Service Act*, and other Acts of Parliament, including *the Competition Act*.

The CC and these Acts provide law enforcement and national security agencies with powers to intercept communications, and search for and seize information in a manner consistent with the rights guaranteed in the *Canadian Charter of Rights and Freedoms*, particularly the right to be secure against unreasonable search and seizure. Updating lawful access legislation has been on the government agenda for some time but successful passage of legislation has yet to occur, hence the tabling of the current Bill C-XX. Key reasons updated lawful access legislation is needed include:

- Canada's legislation on this matter is antiquated and has not kept pace with the rapid evolution of technology.
- The RCMP and other law enforcement agencies face situations where authorizations to intercept communications cannot be readily executed due to a lack of technical capability for interception in telecommunications service providers' networks.
- Access to basic subscriber information is often required in the early stages of investigations and is essential for pursuing investigative leads. Lack of timely access to this information can delay or possibly block investigations and undermine public safety and security.
- Basic subscriber information simply provides police with a starting point in an investigation; obtaining identifying information such as a person's name and address is tombstone information. To advance an investigation, warrants will still be required.

Strategic Consideration
The fact that three Bills have now been combined into one may serve to complicate what was already complex when the Bills were separate.

Media lines

- The proposed legislation and amendments to the *Criminal Code* would provide more effective tools to investigate criminal acts in the digital age.
- The RCMP believes police need modern tools and resources to respond to the evolving nature of national and transnational crime, including terrorism.
- Hi-tech criminals are using state of the art technology to carry out illegal activities – to undertake crime, to conceal activities and to communicate securely with associates. Law enforcement is often hamstrung using legal tools dating from the 1970s and 80s.
- Police require lawful access to communications and information in a number of instances including investigations into organized crime, drug trafficking, terrorism, and online child sexual abuse.
- The proposed updates to lawful access legislation maintain appropriate judicial oversight required to protect the privacy of Canadians in accordance with the Charter.
- Lawful access laws balance the privacy rights of Canadians and the public interest in police having modern and effective tools and capabilities to investigate crime and protect public safety.
- New lawful access legislation will bring Canada in line with many other countries which already have similar laws including the United Kingdom, the United States, Australia, Germany and Sweden. Canada and Japan are the only G-8 countries without intercept capability legislation.

Basic Subscriber Information (Customer Name and Address)

- The type of basic identifying information that could be requested by police under the proposed legislation includes only subscriber name and address, telephone number or e-mail address, local service provider identifier, and Internet protocol address. It is such rudimentary information that it attracts no - or a very minimal - expectation of privacy.

- Canadians disclose their BSI publicly on a daily basis. This is especially true today with the popularity of social networking sites. BSI is today's electronic equivalent of the telephone books

- Police require basic subscriber information (BSI) in their daily work. Investigations in which police may need to request BSI include:

    - Child sexual exploitation;
    - Drugs and organized crime;
    - Abduction/missing persons;
    - Fraud/financial crime;
    - Others i.e., notifying next-of-kin after a car accident and addressing suicide threats over crisis lines

- BSI is no different from police searching a vehicle's plate number to find out who the registered owner is.

- Access to basic subscriber information is often required at the early stages of investigations and is essential for pursuing investigative leads. Lack of timely access to this information can delay or block investigations and undermine public safety and security.

- Currently in Canada, ISPs are allowed under the Personal Information Protection and Electronic Documents Act (PIPEDA), to voluntarily (but are not obligated to do so without warrant) provide basic subscriber information without warrant. Consequently, they can and often do, refuse to cooperate with law enforcement. Without this basic information as a starting point, law enforcement may face roadblocks which can hamper an investigation.

- Some service providers release basic subscriber information to authorities upon request, others fail to provide it in a timely fashion, and still others insist on a warrant. There are situations where obtaining a warrant for this basic information is neither practical nor possible and the result is criminals escape justice. Lawful access will address the lack of uniformity in the process across Canada.

- Requiring ISPs and TPSs to provide basic subscriber information to police will help authorities follow the necessary steps to confirm the identity of individuals suspected of committing crimes.

- Law enforcement needs BSI to pursue investigations at their earliest stages. Giving BSI to law enforcement upon request and without a warrant will by no means give law enforcement the contents of a suspect's computer for instant message trails, Internet surfing records, or banking or medical information without a warrant.

Intercept

- Current legislation does not require telecommunications companies to build in intercept capabilities. Bill C-XX would ensure that over time, companies build these features into their systems.
- By requiring telecom service providers (TSP's) to have intercept-capable equipment, the legislation will ensure that when police are legally authorized to intercept communications, they are able to rely on the technical capability of the TSP to do so.

Questions and Answers

Q. 1. Why does the RCMP need the additional powers proposed as part of the government's lawful access legislation?

A. The proposed legislation does not provide for any additional police powers with respect to the lawful interception of communications. Currently, there is no requirement for telephone and Internet companies to develop and maintain systems that provide intercept capability. This means that when the courts give the police (or CSIS) the authority to do an intercept (wiretap), many service providers do not have the technical capability to comply with the court order. As a result, the police and CSIS often have to spend a considerable amount of time and resources researching and developing new methods to gain lawful access to these communications networks. Criminals and terrorist groups are able to take advantage of this to hide their illegal activities, and as a result, put public safety at risk.

Q. 2. Didn't police say in the past that such legislation would provide them with no new powers? What's changed?

A. Nothing has changed. The proposed legislation does not provide for any additional police powers with respect to the lawful interception of communications. But now that the proposed legislation is in the form of an amalgamated or omnibus bill, it also includes some updated or modernized investigative tools, for example under the *Criminal Code* amendments.

Q. 3. Doesn't this legislation give the RCMP the power to monitor websites and individual visits without a warrant?

A. No. Tracking a subscriber's activities on the Internet would not be authorized under the *Act.* Law enforcement will still require a warrant from the courts to obtain this type of information, or the contents of any communication.

Q. 4. In the case of the basic subscriber information you're asking for, what is this, why do you need the information and exactly how do you use it?
A. Subscriber information provides police a starting point in an investigation or helps them to carry out general (non-investigative) duties, such as notifying next of kin about a serious accident or returning stolen property. A person's name and address is rudimentary – it's what police call "tombstone" information. Today, if you drive away from the scene of an accident, police find your name and address by looking up your license plate. This is no different. Without subscriber information, police could be left with no avenues to pursue a possible criminal case.

Q. 5. You've said that even without updated legislation, accessing basic subscriber information does not require a warrant. Then why do you need these changes and why do some ISPs demand police obtain a warrant before they (the ISPs) release subscriber information?
A. Some ISP's are refusing to disclose CNA information without a warrant. Doing so can unnecessarily delay and hamper an investigation.

The reason is a statute called PIPEDA (Personal Information Protection and Electronic Documents Act). This Act governs the collection, use, and disclosure of "personal information" by federally-regulated companies such as telcos and ISPs. It gives them the discretion (choice)

to provide non-sensitive personal info (e.g. basic identifying information) to police for an investigation. This is the type of information that doesn't attract Charter protection and so doesn't require a court order to be lawfully obtained. Some ISPs refuse to release BSI without a warrant even though they have the discretion to do so under PIPEDA.

Includes revisions from

Brigitte Mineault (CPCMEC)	17 Nov
Bernie Tremblay (Tech Crime)	18 Nov
Helen Van Dyk (Legal)	23 Nov
Susan Alter (Legal)	26 Nov

Prepared by:
Jim Spendlove, Team Lead, PSS,
National Communication Services

Approved by: pending
Bernie Tremblay
Helen Van Dyke
Susan Alter
Marc Flynn
Yves Desjardins
Joe De Mora
Marc Richer

From: Brigitte Mineault
To: Konarski, Tom; Piche, Pierre
Date: 9/14/2009 11:06 AM
Subject: lawful access Op-Ed

scan

Tom and Pierre,

Please see below the Op-Ed the Minister's office want to send out. Any concerns with this please let me know.

Merci

Brigitte Mineault
Communications Team Lead, Policing Support Services/Chef d'équipe en Communications, Soutien aux Services de Police

National Communications Services /Services Nationaux de Communication
RCMP/GRC
Tel: 613-949-0285
Cell: 613-298-9264

>>> Liam Gerofsky 9/11/2009 4:46 PM >>>
Hi Meredith,

We don't see any immediate concerns, but are still checking with the SMEs.

Liam

-----Original Message-----
From: "Burton, Meredith" <Meredith.Burton@ps-sp.gc.ca>
To: Maureen.McGrath@ic.gc.ca <Maureen.McGrath@ic.gc.ca>
To: Butcher, Joan <JButcher@justice.gc.ca>
Cc: Savoy, Jennifer <Jennifer.Savoy@ps-sp.gc.ca>
To: Gerofsky, Liam <Liam.Gerofsky@rcmp-grc.gc.ca>
To: Spendlove, Jim <Jim.Spendlove@rcmp-grc.gc.ca>

Sent: 11/09/2009 3:16:23 PM
Subject: FYI Op-Ed

Hi everyone. FYI, our Mino is considering issuing an op-ed in response to comments by the privacy commissioners. Please see below. If you have concerns, please advise.

Cheers,
Meredith

Op-Ed - Bill C-47

I would like to respond to some remarks made by the Federal, Provincial and Territorial Privacy Commissioners. While I have great respect for the work they do, I feel there have been some misunderstandings about Bill C-47, the Technical Assistance to Law Enforcement in the 21st Century Act. As such, I believe clarification is needed.

First, let's start with what Bill C-47 is not: It is not about intercepting or eavesdropping on the private communications of Canadians. Nor is it about monitoring the web surfing habits of Canadians or preventing them from sending anonymous e-mails.

The proposals in Bill C-47 are about ensuring that law enforcement can keep up with new communication technologies and continue to implement warrants authorized by the courts. New technology is a powerful tool however, in the hands of criminals and terrorists, this technology can be used in ways that threaten public safety. The Government of Canada needs to update Canadian laws to keep pace with new technology - a step already taken by many of our international partners.

I want to be clear: The legislation provides no new powers to intercept communications. The existing requirements for judicial authorization for intercepts will be maintained. Since 1974, police in Canada have been authorized to intercept private communications when a court order is issued by a judge who believes on reasonable grounds that a serious offence, such as child pornography, drug trafficking, money laundering or murder, has been or will be committed. The judge must also be satisfied that authorizing the intercept is in the best interests of the administration of justice and that other investigative procedures have been tried and failed.

Nothing proposed in Bill C-47 will change these limits. Nor will it upset the strong balance established between the protection of privacy, human rights and the safety of our citizens, which are values we all cherish.

Today, telephone and Internet companies are not required to build intercept capabilities into their networks. Because of this, even with a court order, police may not be able to intercept communications. Under Bill C-47, communications providers would be required to update their systems to enable interceptions approved by the courts. To avoid undue burden, the proposed law would allow companies to build this capability gradually over time.

There have also been misunderstandings about the Government's proposals for police and CSIS to obtain subscriber information. Basic subscriber information such as a customer's name, address, telephone number and Internet address can be valuable at the initial stages of an investigation.

The problem is that while some service providers give subscriber information to law enforcement upon request, others fail to provide it in a timely fashion, or refuse to provide it at all. This has created a difference in industry practices across the country.

Access to subscriber information is particularly important in the online context, as criminals use the internet to operate with anonymity. For example, in cases where a child is lured over the internet by a sexual predator, often the only clue police have as to the identity of the perpetrator is an IP address associated with a chat room. In these situations, police need to quickly establish the identity of the suspect based on the IP address. In several cases, service providers have refused to share this information, thereby leaving some children at risk. This proposed legislation will help to ensure that there are no more dead-end investigations.

The proposed legislation would require telephone and internet companies to provide this information to designated law enforcement and CSIS officials without a warrant. Bill C-47 includes some of the very safeguards identified by the privacy commissioners to protect privacy, such as the requirement to track who is requesting the information and why, to permit audit and oversight of how the information is handled, and a five year Parliamentary review.

Canadians can rest assured that any updates to our legislative regime will respect the privacy and human rights entrenched in laws such as the Canadian Charter of Rights and Freedoms, the Privacy Act, and the Personal Information Protection and Electronic Documents Act.

Senior advisor / Conseillère principale
Communications - Emergency Management and National Security
Sécurité nationale et gestion des urgences - Communications
Public Safety Canada / Sécurité Publique Canada
Tel: 613-949-6583
Cel: 613-219-1285
Fax: 613-993-7062
meredith.burton@ps-sp.gc.ca

From: "Kwavnick, Andrea" <Andrea.Kwavnick@ps-sp.gc.ca>
To: 'Susan Alter' <Susan.Alter@rcmp-grc.gc.ca>
CC: "Kousha, Hasti" <Hasti.Kousha@ps-sp.gc.ca>, Bernard Tremblay <Bernard.Tremblay@rcmp-grc.gc.ca>
Date: 12/7/2009 2:15 PM
Subject: RE: Next Ops Fees Meeting

Hi Susan,

The CACP proposals in the Nov 2009 documents are older proposals that they had brought forward before. And as you have stated, the proposals were discarded. I will provide the partners with the related documentation.

Thanks
Andrea

-----Original Message-----
From: Susan Alter [mailto:Susan.Alter@rcmp-grc.gc.ca]
Sent: December 7, 2009 2:08 PM
To: Kwavnick, Andrea
Cc: Kousha, Hasti; Bernard Tremblay
Subject: RE: Next Ops Fees Meeting

Hi Andrea,

Thanks!
Susan

>>> "Kwavnick, Andrea" <Andrea.Kwavnick@ps-sp.gc.ca> 12/7/2009 12:38 PM
>>> >>>
We will be staying with 1:30 for this week's meeting, at which time we can discuss our meeting schedule.

I am attaching recent documents released by the CACP. I would like to discuss their position on Ops Fees (q. 3 of the Q&As) on Thursday.

Thanks
Andrea

From: Kwavnick, Andrea
Sent: December 7, 2009 10:25 AM
To: Kwavnick, Andrea; 'Susan Alter'; 'Bill Milley'; 'Pierre Piche'; 'Bernard Tremblay'; 'Derm Coombs'; 'Gordon Kirk'; 'Mike BOURQUE'; Kousha, Hasti; Fobes, Caroline; 'kaudcent@justice.gc.ca'; Dincoy, Rana; Shannon, Matthew; Goodwin, Darlene
Subject: RE: Next Ops Fees Meeting

Colleagues,

Hasti has informed me of a scheduling conflict, in that she will be required to attend another set of

meetings held every Thursday afternoon.

Would there be a scheduling conflict for any members of the group if we were to move our meetings to Thursday mornings at 10:00, beginning with our December 10th meeting?

Please let me know at your earliest convenience, so that we know how to proceed.

Thanks
Andrea

From: Kwavnick, Andrea
Sent: December 1, 2009 3:53 PM
To: 'Susan Alter'; Bill Milley; 'Pierre Piche'; Bernard Tremblay; Derm Coombs; 'Gordon Kirk'; 'Mike BOURQUE'; Kousha, Hasti; Fobes, Caroline; 'kaudcent@justice.gc.ca'; Dincoy, Rana; Shannon, Matthew; Goodwin, Darlene
Subject: Next Ops Fees Meeting

I would like to hold our next meeting on Thursday, December 10th at 1:30 at 340 Laurier (11E).

I would like to thank the partners for their comments on the Ops Fees Policy Principles document. These comments have been incorporated into the document, which I am sending out again. We can discuss further at our next meeting. Once we have the principles agreed upon, I think it is important to present to Industry and Treasury Board.

Thanks
Andrea

CACP Key Messages – Lawful Access Legislation
Updated November, 2009

Definition:

- 'Lawful Access' refers to the lawful interception of private communications by law enforcement and national security agencies.

CACP Goal

- The goal of the Canadian Association of Chiefs of Police is to see government modernize legislation to help police detect and prevent crime and apprehend criminals who seek to exploit electronic communications to the detriment of society.

History:

- The CACP has been advocating for electronic interception laws or what is commonly referred to as the "Lawful Access" initiative.
- In the age of cell-phones, Blackberries and the Internet, police in Canada are operating under laws written when rotary phones were the norm.
- Bills C-46, Investigative Powers for the 21st Century Act and C-47, Technical Assistance for law Enforcement in the 21st Century Act have passed second reading in the House of Commons and has been referred to the Standing Committee on Public Safety and National Security.

Parameters:

- This legislation is NOT about increasing police powers. It is about addressing the current and growing gap between our current laws and the reality of new and emerging technologies.
- There should be no "intercept safe havens" for criminals in Canada. Technology companies should have the technological ability to implement court-ordered lawful access orders.

Modern challenges facing Canadian law enforcement that are driving the need for reform

- Police investigations are increasingly complex, extensive, expensive and time and resource intensive. Court ordered interceptions are a vital investigative tool used in the most serious and complex of investigations.

- Organized criminals, internet predators, cyber-criminals, and terrorists are aware of, and benefit from modern communications technologies which operate free of geographical constraints.

- Changes to lawful access legislation are long overdue. Technology continues to change and evolve at an unprecedented pace (e.g. text messaging, email, other secure communications, wireless communications, private servers, enhanced encryption etc.) Legislation has not kept pace with these changes. This has proven to be a hindrance to law enforcement and national security agencies.

Required Legislative Changes:

- Modernization of Canada's electronic surveillance legislation is critical. Current provisions do not reflect the reality of evolving technology; they are inadequate to allow efficient and effective lawful access to current and emerging data communications services in Canada.

- Current laws related to lawfully authorized access to communications require modernization. Virtually every western democracy, including Australia, New Zealand, and the United Kingdom has adopted such legislation.

- Telecommunications and internet service providers should include interception capability in all new technologies they are releasing.

Customer Name and Address Information (CNA):

- The ability to access basic subscriber information is a critical component of many police and national security investigations. Currently, there is inconsistency and uncertainty in accessing this kind of information.

- CNA information refers to such basic personal identifiers as the name and address associated with a phone number and the company that is providing service to a given phone number or Internet (IP) address Additional information can only be secured with prior judicial authorization.

- Timely access to basic subscriber information, held by telecommunications and internet services providers, is non-intrusive and is a key 'building block' for successful investigations.

  Case law seems to support the proposition that police may access this data without judicial authorization. Most privacy statutes presently permit such disclosure to law enforcement and national security agencies.

- The procedures and requirements for accessing CNA information would benefit from being standardized and consistent across the country. Record-keeping and audit

requirements would provide – indeed improve any existing - procedural and accountability safeguards.

- The CACP supported the *Modernization of Investigative Techniques Act (MITA)* that was tabled in 2005. The well-researched provisions in that Act allowed for access to CNA information without prior judicial authorization under a regime of legislated accountability provisions.

- Canadian law enforcement supports the need to obtain search warrants for lawful interceptions when they are legally required. They are not demanding a widespread "warrantless search regime".

Communications Meeting – IPCECA 2011-11-01

(Yves, Mark, Hélène, Simon, J-S., Bernie)

- Message Event Proposal
  - RCMP – interception expert (technical side of interceptions)
    CPC MEC (Billinski ?) Supt.

- Media could not tech. Q's. Speakers won't be quoted by name, although the info provided can be quoted.
- Followed by Media event (news conference) where ministers will speak (likely not RCMP)

Simon suggestion: an old example of intercept capability (about technology that is not a problem anymore)
: CVA example

- No new interception powers, but there are new CVA powers (powers to compel)

For committee, will need senior officials

Focus on Big-picture!

- No warrant required (no. REP)
- IP address web info → lead order with delay
- (A) No offence or (B) No RGD to support → lead order + data (from 6306) + express

* attach examples for each situation

Privacy Commissioner has been discussed / consulted in the past.

Be clear on :- what information we are after (detail what the PSII is)
- why we need that info. how is it helpful to us.
- address the gateway info argument ⇒ Some feel once we get CVA, we can move on to others ⇒ focus on info need still in most of these cases

CSIS and Competition Bureau ⇒ they should speak up about need for IP address in s. 16 as a gate e.g. community web mind + false name. Could ask for IP from which they logged in from. Then go to TBP for CVA (this goes further than what we do now and many others greater REP).

⇒ Suggest story timeline with devices re: when PSII came in, 2004 ago, now, future...
from 1974

- For press conference there may be ~~does~~ rehearsal

"Media Lines" (PS) document is not planned to be used
- Post regime will evolve

Qs to address:
- See issues in Priv. Comm's letter to minister
  - BSI concerns re: necessity (need for the provisions)
    - Necessity, proportionality, safeguards, effects on people
- Why we now need to compel TSPs to give CNA

To do

RCMP big picture with all terms + add numbers + examples (CSIS with preamble, picture, apps)

RCMP Q's & A's → Jim will pull material for RCMP lines from what he has (we will review + add/amend if necessary)
- PIPEDA → allows it already (C-52 with added safeguards)
- In US "NSL Letters" we closed in 30 % of cases → we will have stronger safeguards

PIPEDA amendments have already been tabled

Collect:
- authorized by law
- Level is minimal
- executed in a manner that is reasonable.

} Issue: What line of thinking to eliminate that it is OK to obtain (CSIS even if they cannot put forward a CEP) without warrant.

R will send examples and stats to Maciek. Jim will send to PS comms.

SME for BSI/CNA

ANALYSIS OF

Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials on Bills C-46 and C-47

Scan

("Protecting Privacy for Canadians in the 21st Century")

September 9-10, 2009, St. John's, Newfoundland and Labrador

CONTEXT

1. The federal government tabled two pieces of legislation in June 2009 aimed at giving Canadian law enforcement, national security agencies and others (hereafter referred to as "authorities") broader powers to acquire digital evidence to support their investigations.

2. Bill C-46, the *Investigative Powers for the 21st Century Act* (IP21C), would allow authorities to order telecommunications providers to preserve and turn over the details of their subscribers' communications. Authorities would also have the power to apply for special orders to trace mobile communications devices and, by extension, their owners.

3. Bill C-47, the *Technical Assistance for Law Enforcement in the 21st Century Act* (TALEA), would give authorities access to information about subscribers and their mobile devices, even without a warrant. The bill would also oblige all telecommunications companies to build in a capability allowing authorities to intercept communications on their networks.

4. The provisions of the proposed Acts raise privacy concerns. For instance, without a warrant, authorities could gain access to personal information such as unlisted telephone numbers, and e-mail and IP addresses.

5. Canadians consider much of this personal information to be sensitive and expect it to be kept confidential.

6. Canadians also expect their use of computers and mobile devices to remain private.

7. The legislation as currently drafted is not limited only to investigations of serious criminal offences, but also could be used to target even minor infractions and non-criminal matters.

WHEREAS

1. Privacy is a fundamental human right that enables the freedom of association, thought and expression.

2. Canadian courts have consistently affirmed the importance of these rights.

3. Canada has a legal regime governing the use of surveillance that protects individual rights while also giving authorities access to communications when authorized. This framework has been carefully refined over decades by Parliament and the courts.

4. To date, the federal government has presented no compelling evidence that new powers are needed.

THEREFORE

The Federal, Provincial and Territorial Privacy Commissioners of Canada urge Parliament to ensure that the proposed legislation to create an expanded surveillance regime strikes the right balance between individual privacy and the legitimate needs of the authorities by:

1. Approaching IP21C and TALEA with caution because they alter a carefully constructed and workable framework;

2. Obliging the government to demonstrate that the expanded surveillance powers they contain are essential and that each of the new investigative powers is justified;

3. Exploring the alternative that, should these powers be granted, they be limited to dealing with specific, serious crimes and life-threatening emergencies;

4. Ensuring that any legislative proposals on surveillance:

    a. Be minimally intrusive;

    b. Impose limits on the use of new powers and ensure appropriate legal thresholds remain in place for court authorization;

    c. Require that draft regulations be reviewed publicly before coming into force;

    d. Include effective oversight;

e. Provide for regular public reporting on the use of powers; and

f. Include a five-year Parliamentary review.

From: "Burton, Meredith" <Meredith.Burton@ps-sp.gc.ca>
To: "Dincoy, Rana" <Rana.Dincoy@ps-sp.gc.ca>, "Fobes, Caroline" <Caroline.Fobes@ps-sp.gc.ca>, "Kwavnick, Andrea" <Andrea.Kwavnick@ps-sp.gc.ca>, "Shannon, Matthew" <Matthew.Shannon@ps-sp.gc.ca>, "Goodwin, Darlene" <Darlene.Goodwin@ps-sp.gc.ca>, "Thompson, Julie" <Julie.Thompson@ps-sp.gc.ca>, "Spendlove, Jim" <Jim.Spendlove@rcmp-grc.gc.ca>, 'DanOlson' <Dan.Olson@rcmp-grc.gc.ca>, '"Butcher, Joan"' <JButcher@justice.gc.ca>
CC: "MacDonald, Michael" <Michael.MacDonald@ps-sp.gc.ca>, a>, "Coburn, Stacey" <Stacey.Coburn@ps-sp.gc.ca>
Date: 4/9/2010 4:40 PM
Subject: Movement on lawful access / talea
Attachments: 2010-04-09 lawful access NR updated.doc; 2010-04-09 lawful access ML v1.doc ; 2010-04-09 BK Lawful access.doc; 2010-04-09 Qs and As_POLICY.doc

Rumours of an imminent tabling for lawful access/talea legislation are now more credible, with the latest word coming from Andrew House that this could be re-introduced in the House the week of April 19. The precise date is still unknown.

For your review, the products developed for the bill last year, with updates tracked in the documents.

I realize it's short notice, but I would appreciate hearing from you no later than COB April 13, so that we can incorporate your changes in our final approvals.

Thanks,
Meredith

A/Manager / Gestionnaire pi
Communications - Emergency Management and National Security
Sécurité nationale et gestion des urgences - Communications
Public Safety Canada / Sécurité Publique Canada
Tel: 613-949-6583
Cel: 613-219-1285
Fax: 613-993-7062
meredith.burton@ps-sp.gc.ca

Public Safety Canada / Sécurité publique Canada

Media Lines

ISSUE: On April xx, 2010, the Government of Canada introduced Bill C-xx, the *xxx Act*, to support the interception of communications by law enforcement agencies and CSIS by requiring intercept capability in telecommunications networks. The law will also provide law enforcement agencies and CSIS with access to basic subscriber information. This legislation had been previously introduced as (name and C-xx) on June 18, 2009, but it died on the Order Paper when the House was prorogued December 30, 2009. .

MEDIA LINES:

- The Government of Canada is committed to the safety and security of Canadians and their communities.
- This legislation will help keep Canadians safe from those who would use new communications technology to pursue criminal or terrorist activities.
- The *XX Act* ensures that law enforcement can keep pace with new communication technologies and continue to execute judicially authorized warrants.
- The legislation provides no new powers to intercept communications. The warrant processes for the interception of private communications will not change with this Bill.
- It will also provide for a balanced and well-regulated administrative regime for the disclosure of basic subscriber information to law enforcement and CSIS when requested.
- Canada is joining many other countries including the United Kingdom, the United States, Australia, Germany and Sweden, which already have similar laws for interception and the sharing of basic subscriber information.

If asked about interception:

- This Government is committed to providing law enforcement and national security agencies with the tools they need to prevent, investigate and prosecute serious crimes including terrorism.
- While technology has advanced over the past two decades, the capability of police to lawfully intercept communications has not kept pace.

Canada

Government of Canada / Gouvernement du Canada

News Release

GOVERNMENT OF CANADA INTRODUCES LEGISLATION TO UPDATE TOOLS TO FIGHT CRIME AND TERRORISM

OTTAWA, April xx, 2010 – The Honourable Vic Toews, Minister of Public Safety today introduced in the House of Commons an important piece of legislation to ensure law enforcement and national security agencies are equipped to fight crime and terrorism in today's high-tech environment.

"New technology is a powerful tool, however in the hands of criminals and terrorists, this technology can be used in ways that threaten public safety," said Minister Toews. "The Government of Canada needs to update Canadian laws to keep pace with new technology – a step already taken by many of our international partners."

The proposed legislation will ensure that law enforcement can keep up with new communication technologies and continue to implement warrants authorized by the courts. While technology has advanced rapidly in the past two decades, increasingly law enforcement and national security agencies have faced technical obstacles to protecting the safety and security of Canadians. .

The *XXXX Act* requires service providers to include interception capability in their networks. Since 1974, police in Canada have been authorized to intercept private communications when a court order is issued by a judge who believes that a serious offence, such as child pornography, drug trafficking, money laundering or murder, has been or will be committed. Requirements to obtain court orders to intercept communications will not be changed by this Act, which will also require service providers to supply basic subscriber information to law enforcement agencies and the Canadian Security Intelligence Service on request.

Other countries, such as the United Kingdom, the United States, Australia, New Zealand, Germany and Sweden, already have similar legislation in place.

The Government considered input from a broad range of stakeholders in developing the legislation, including the telecommunications industry, civil liberties groups, victims' advocates, police associations and provincial/territorial justice officials. Bill C-xx strikes a balance between the need to protect the safety and security of Canada, the competitiveness of the telecommunications industry, and the privacy rights of Canadians.

An online version of the legislation will be available at www.parl.gc.ca.

Canada

Public Safety Canada / Sécurité publique Canada

Backgrounder

BACKGROUNDER

XXX Act

INTERCEPT COMPONENT

The interception of communications is essential for investigating and prosecuting serious crime and combating terrorism. Police forces and the Canadian Security Intelligence Service (CSIS) require lawful access to communications in a number of contexts, including investigations into child sexual abuse, organized crime, drug trafficking, and terrorism.

The *XXX Act* will not provide law enforcement or CSIS with any new interception powers, nor will it change or expand existing interception authorities in any way. Rather, it will address the challenges posed by modern technologies that did not exist when the legal framework for interception was designed nearly 40 years ago. Police forces and CSIS will continue to require warrants for interception. This legislation will simply ensure that when warrants are issued, a technical solution is available so that police forces and CSIS can actually intercept communications.

Canada currently has no legal requirement for companies to build interception capability into telecommunications networks. As a result, we now have situations where judicial authorization is granted (a warrant is issued), but cannot be effected because the service provider's network is not intercept capable. Criminals and terrorists are aware of interception "safe havens" and exploit them to continue their criminal activities undetected. As new telecommunications services and products are being rolled out every day, police forces and CSIS continue to fall behind increasingly sophisticated criminal and terrorist groups. There are far too many instances where police forces and CSIS cannot execute judicially authorized interceptions to protect Canadians' safety, simply because of a lack of intercept capability on telecommunications networks.

A technical solution will now be available for police forces and CSIS to execute judicially authorized warrants.

The proposal will require companies to pay for intercept capability in certain new equipment and software, while the Government will provide reasonable compensation when retrofits to existing networks are needed – this is a shared response to a problem that directly affects the safety of Canadians.

Along with sharing the cost of fixing this problem, we have built flexibility into the legislation. For example:

- A number of entities (such as banks, private networks, and charities) are excluded from the legislation's requirements, and will not be required to

Canada

have intercept capability.

- A three-year exemption will be granted to "small" service providers (those with less than 100,000 subscribers) from certain requirements deemed too costly for them at this time. After the three years, these companies will be expected to fully comply with the requirements of the legislation.

- Upon approval by the Government, exemptions may be granted to service providers for two-year periods, with conditions, to permit innovative technologies to be brought to the marketplace prior to being fully compliant with the requirements of the Act. This will allow service providers to remain competitive in the global marketplace, while developing intercept solutions for these new technologies.

- Service providers will also be free to select the most cost-effective intercept solutions available, and will not be tied to government-determined standards or equipment.

This flexible and gradual approach will avoid placing an undue burden on industry, while at the same time ensuring that telecommunications service providers build and maintain interception capability on a going-forward basis. In doing so, this legislation strikes the right balance between the needs of police forces and CSIS, the safety and security of Canadians, and the competitiveness of industry.

Nothing in this legislation will diminish the considerable legal protections currently afforded to Canadians with respect to privacy or freedom from unreasonable search and seizure.

SUBSCRIBER INFORMATION COMPONENT

Police forces and CSIS also require timely access to basic subscriber information as it is an essential tool for fighting crime and terrorism. Subscriber information refers to basic identifiers such as name, address, telephone number and Internet Protocol (IP) address, e-mail address, service provider identification and certain cell phone identifiers. These basic identifiers are often crucial in the early stages of an investigation, and without this basic information, police forces and CSIS often reach a dead-end as they are unable to obtain sufficient information to pursue an investigative lead or obtain a warrant.

Currently, there is no legislation specifically designed to require the provision of this information to police forces and CSIS in a timely fashion. As a result, the practices of releasing this information to police forces and CSIS vary across the country: some service providers release this information to law enforcement immediately upon request; others provide it at their convenience, often following considerable delays; while others insist on law enforcement obtaining search warrants before the information is disclosed. This lack of national consistency and clarity can delay or block investigations.

Technical Assistance for Law Enforcement in the 21st Century Act

Questions and Answers

TABLE OF CONTENTS **Page**

TECHNICAL ASSISTANCE FOR LAW ENFORCEMENT IN THE 21ST CENTURY ACT
Qs & As

LAWFUL ACCESS - GENERAL

Why do we need to update lawful access legislation?

- *Criminal Code* provisions regarding the interception of communications date back to 1974.
- Canada's legislation has not kept pace with the rapid evolution of technology.
- The Canadian Security Intelligence Service (CSIS) and police currently face situations where interception warrants can't be executed due to a lack of technical capability in the telecommunications service providers' networks.
- Criminals and terrorists are aware of interception "safe havens" and exploit them to continue their activities undetected. This legislation is necessary to eliminate those "safe havens".

What is proposed in the new legislation?

- The *Act* will require telecommunications service providers to build and maintain intercept capable networks by ensuring that new and significantly modified technologies are intercept capable.
- The *Act* will also introduce much needed consistency and protections for the release of basic subscriber information.
- The *Act* will also clarify that telecommunications service providers must provide this information to designated police, CSIS and Competition Bureau officials upon request.

What is the difference between the Department of Justice's Bill C-XY (formerly Bill C-46) and Public Safety's Bill C-XX (formerly Bill C-47)?

- While both Bills are designed to provide law enforcement with the tools they require to keep Canadians safe in the 21st century, the Bills are designed to do this in different ways.
- Bill C-XY will amend elements of the *Criminal Code* and other statutes to better address cybercrime and crimes committed using new technologies. These amendments will provide law enforcement with an enhanced tool kit for acquiring digital evidence.
- Bill C-XX will obligate telecommunications service providers to have the capability to implement interceptions and to provide basic subscriber information to the police, CSIS and the Competition Bureau upon request.

INTERCEPTION CAPABILITY

What is lawful interception of communications?

- The lawful interception of communications refers to the ability of police and CSIS to covertly gain access to an individual's private communications through the use of electronic surveillance, when authorized to do so.
- The interception of private communications is illegal under the *Criminal Code* except in those cases where the interception has been legally authorized.
- The *Criminal Code* also contains a number of restrictions on the use of this power. For example, section 183 of the *Criminal Code* limits the types of offences for which an application for an authorization to intercept private communications can be sought.

Are you giving police new interception powers?

- No, the *Act* is not about giving new interception powers.
- The *Act* is about addressing the technical obstacles that prevent the police from using their lawful authorities.

Why do police and CSIS need this legislation?

- Currently, there is no requirement for telephone and Internet companies to develop and maintain systems that provide interception capability.
- This means that when the courts give the police and CSIS the authority to do an intercept, many service providers do not have the ability to comply with the court order.
- The police and CSIS often have to spend a considerable amount of time and resources researching and developing new methods to gain lawful access to these communications networks.
- Criminals and terrorist groups are able to take advantage of this to hide their illegal activities.

Will there be public reporting on interceptions?

- Public reporting already exists and will not be affected by the proposed *Act*.
- Under the *Criminal Code*, the Minister of Public Safety must publish information regarding the number of authorizations applied for in a given year.
- The Security Intelligence Review Committee provides similar information in its annual report to Parliament with respect to CSIS's activities.

How has this been used in the past?

- Lawful access is an essential tool in the prevention, investigation and prosecution of serious crimes and terrorism. For example:
    - In 2006, lawful access was critical to the investigation and arrest of over a dozen suspected terrorists in the Toronto area.
    - In 2007, lawful access supported the arrest of almost 100 individuals involved in organized crime and helped solve 13 murder cases involving these people.

SUBSCRIBER INFORMATION

What is subscriber information?

- Subscriber information refers to the basic information about a customer that is held by a telecommunications service provider.
- It is comprised of a subscriber's name, address, telephone number, and if applicable, email and Internet Protocol (IP) addresses, and/or certain cellular telephone identifiers.
- It does not include any information pertaining to the websites a person visited, the contents of their emails, or the phone calls they either made or received.

Why do police need subscriber information?

- The police require timely access to subscriber information in a wide variety of situations, ranging from performing general policing duties to investigating serious threats to the safety and security of Canadians.
- Access to subscriber information is particularly relevant in the online context, as criminals use the Internet to operate with anonymity.
- For example, in cases where a child is lured over the Internet by a sexual predator, often the only clue police have as to the identity of the perpetrator is an IP address associated with a chat room.
- In these situations, police need to quickly establish the identity of the suspect based on the IP address.
- Examples of situations where subscriber information is used by police include:
    - investigating the sexual exploitation of children;
    - investigating Internet fraud and other online crimes;
    - identifying an incapacitated person carrying only a cell phone to notify next of kin;
    - providing police with a car accident victim's civic address, in situations where only the rural address of the victim is known via the victim's driver's license;
    - addressing suicide threats over crisis lines; and,
    - returning stolen property to its rightful owner.

How is subscriber information currently accessed?

- Currently, a warrant is not needed to access basic subscriber information.
- No legislation exists to specifically address the release of basic subscriber information to the police and CSIS.
- That is why, today, practices vary across the country. Some providers release information immediately upon request; others provide it at their convenience, often following considerable delays; while others insist on warrants.
- Today, there is no required record keeping of requests and no system of accountability.
- Bill C-XX is designed to address these inconsistencies.

What is wrong with the current regime of access to subscriber information?

- The current regime operating today lacks consistency and clarity. This lack of consistency and clarity can delay or block crucial investigations.
- This *Act* would create clarity regarding the responsibility of service providers to disclose basic subscriber information to the police, CSIS and the Competition Bureau upon request.
- While this *Act* is in line with the existing practice of not requiring a warrant, it proposes a system of consistency, accountability, record keeping, controlled access, and review, that does not currently exist.

Why can't the police get a warrant every time they need subscriber information?

- Subscriber information is often required at the beginning of an investigation and is considered to be "pre-warrant" information and is often the first and most basic piece of information needed to obtain a warrant.
- Warrants are generally granted for criminal investigations where the identity of the suspect has been clearly established.
- In addition, the police are sometimes faced with situations where they may have reasonable grounds to believe a crime has been committed, but cannot obtain a warrant because they cannot identify the suspect or location of the crime.
- Requiring a warrant for access to basic subscriber information is also 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;
- an individual whose home has been broken into; or,
- family of an Alzheimer's patient who has wandered off.

- There are other cases where acquiring a warrant is simply impractical. The warrant application and execution process involves considerable work for investigators and can take many hours (or days) to complete. In many cases, completing this process would compromise or even jeopardize an investigation.

- A warrant regime would also place an unnecessary burden on the justice system. There are tens of thousands of subscriber information look-ups done annually, at all times of the day and night. The resource and logistics requirements of requiring a warrant in each case would be impractical from an administration of justice perspective.

Under the new regime how many officials could potentially access an individual's subscriber information?

- The legislation stipulates that no more than five individuals or 5% (whichever is greater) of a police force, CSIS and the Competition Bureau may be designated to access subscriber information. This equates to (approximately) :

  - 1,420 officials at the RCMP (28,419 total employees)
  - 150 officials at CSIS (3000 total employees)
  - 23 officials at the Competition Bureau (447 total employees)

Are you giving the police and CSIS the power to monitor websites and individual visits without a warrant?

- No. Tracking a subscriber's activities on the Internet would not be authorized under the *Act.*

- The police will continue to require a warrant from the courts to obtain this type of information, or the contents of any communication.

- The subscriber information to be provided under the *Act* is limited to a subscriber's name, address, telephone number, and if applicable, email and Internet Protocol addresses, service provider identification, and/or certain cellular telephone identifiers. It does not indicate who they called, or which websites were visited.

- The *Act* would not require telecommunications service providers to collect information they do not normally collect as part of their regular business practices, or verify the accuracy of the subscriber information they collect.

- This *Act* would not create a national database of subscriber information.

Did former Public Safety Minister Stockwell Day not publicly endorse an access to basic subscriber information regime with judicial authorization?

- The Government did consider the option of requiring a warrant for access to basic subscriber information and continued to conduct consultations with stakeholders in order to strike the appropriate balance between investigative needs and the rights of Canadians.

- However, feedback from stakeholders demonstrated that a warrant requirement for basic subscriber information would negatively impact the ability to carry out investigations and would introduce an additional burden on the criminal justice system.

- This is an additional burden on police and Crown prosecution's limited resources.

- Basic subscriber information, such as name and address, is often needed at the early stages of an investigation when a warrant could not be obtained.

- Currently, many telecommunications service providers voluntarily provide basic subscriber information for law enforcement and national security purposes. This is permitted under Canada's privacy laws.

- A legislative proposal for access to basic subscriber information with a warrant would impede such voluntary cooperation and significantly impact public safety.

- New privacy safeguards have been included in the legislation to protect personal privacy including limiting access to basic subscriber information to designated officials, and audit and oversight requirements.

APPLICATION AND SCOPE

How many service providers will be affected by this legislation?

- The legislation will apply to all current telecommunications service providers in Canada.
- However, the *Act* was designed in a way that would not impose undue restrictions on telecommunications activities.
- The legislation contains explicit limits to its application, without sacrificing relevance in the face of a rapidly evolving telecommunications industry.
- For example, service providers with fewer than 100,000 subscribers will not have to incorporate intercept capability into new equipment for the first three years of the *Act* coming into force.
- Institutions such as community centers, libraries, restaurants, hotels, apartment buildings or post secondary schools, which offer telecommunications services ancillary to their principal business functions, will have minimal requirements under the proposed legislation.
- Private networks, e-commerce services, e-banking services, elementary and high schools, charities, retirement homes, places of worship, hospitals, and research networks that provide telecommunications services ancillary to their principal functions are excluded from requirements of the legislation.

Would the proposed *Act* put the Canadian telecommunications industry at a competitive disadvantage?

- No, the *Act* will place requirements on all types of telecommunications service providers; this will avoid placing individual sectors or companies at a competitive disadvantage.
- The requirements being placed on the Canadian industry are consistent with those of industry in other countries such as the United States, the United Kingdom, Australia, New Zealand, Germany, Sweden, Finland, the Netherlands, and Spain.

How does this *Act* differ from former Bill C-74, the *Modernization of Investigative Techniques Act*, and Private Member's Bill C-285?

- This *Act* contains several key changes from both former Bill C-74 and Bill C-285, including modification and additions designed to address industry and privacy concerns. These key changes include:
    - provision for payment to service providers for the specialized

telecommunications support and labour they provide in implementing interceptions;

- an extended transition period of 18 months for companies to meet the requirements (formerly a 12-month transition period);
- a five-year Parliamentary review of the legislation;
- an exemption for e-commerce and banking activities;
- a narrowing of the scope of subscriber information to include only those identifiers set out in legislation;
- provision for compensation to service providers for their assistance when providing subscriber information for law enforcement and national security purposes; and,
- clarification to the requirement for companies to decrypt communications they themselves have encrypted.

PRIVACY

How will this *Act* impact personal privacy?

- Today there are protections for private communications in the *Criminal Code* and these protections would not be modified by this *Act*.

- To ensure the appropriate level of privacy protection for the release of subscriber information to the police, CSIS and the Competition Bureau, privacy safeguards have been included in the legislation which do not exist today. This includes:

    - limiting the number of designated officials who may access the subscriber information;
    - mandatory record keeping of all requests for subscriber information;
    - regular audit reports to prevent inappropriate use of the subscriber information; and,
    - limiting the subscriber identifiers to be released to the designated officials.

How have you addressed privacy concerns?

- In the fall of 2007, the Government held targeted public consultations on the issue of police and CSIS access to subscriber information.

- These consultations led to two significant changes designed to strengthen the privacy safeguards contained in the proposed *Act*.

    - First, the scope of identifiers for the subscriber information provisions has been narrowed and limited to only those specified in legislation.

        - This change was made in response to concerns that the scope of identifiers could be easily increased through regulations following the passing of the *Act*.

        - Should authorities seek access to an expanded list of customer identifiers in the future, this would require an amendment to the *Act*, with full Parliamentary debate.

    - Second, the *Act* now includes provision for a mandatory review of the legislation by Parliament after five years. This will help to ensure that the objectives of the *Act* are being met.

        - The Parliamentary review will serve to highlight any unanticipated problems and will provide law-makers the opportunity to amend any parts of the *Act* that are not functioning effectively, including controls on the disclosure of subscriber information.

Will police have to provide a justification for the requests for subscriber information?

- Following consultations, safeguards in the *Act* were expanded to include a requirement for designated officials to ensure the record of the request contains information about the relevance of the information they are seeking to the duty or function they are undertaking, as well as a relevant justification for the request.

Will you be protecting subscriber information from abuse?

- The *Act* respects laws protecting the privacy of Canadians and is consistent with the *Charter of Rights and Freedoms*. It includes safeguards, such as:
    - limiting the number of police and intelligence officers who can request subscriber information (to a maximum of 5% of their organizations);
    - putting procedures in place for mandatory record keeping of all requests for subscriber information;
    - requiring auditing and oversight in order to ensure access to subscriber information is not abused; and,
    - providing that subscriber information is only to be used for the purpose for which it was originally obtained or a use consistent with that purpose.

OTHER COUNTRIES

What are Canada's international partners doing with regard to intercept capability?

- Many other countries, including our allies in the United States, the United Kingdom, Australia, New Zealand, Germany, Sweden, Finland, the Netherlands, and Spain have all recognized the importance of ensuring intercept capability within the communications infrastructure.

- Most of Canada's closest partners updated their lawful access legislation many years ago.

- Given the transnational nature of crime today, many of Canada's allies are now urging Canada to catch up in order to meet our obligations in fighting crime and terrorism.

- The proposals in this *Act* would also assist Canada in fulfilling its G8 commitments with respect to intercept capability.

What are Canada's international partners doing with regard to access to subscriber information?

- Many countries have legislated a requirement to provide this information on request to authorities for law enforcement and national security purposes.

- Administrative models for such access exist in many countries including the United States, the United Kingdom, Germany, Australia, Sweden, Finland, the Netherlands, Ireland, Italy and Norway.

- Bill C-XX provides not only more safeguards for access to subscriber information than exist currently in Canada, but would also provide as many or more safeguards than other Western nations for this type of information.

Why did it take Canada longer than other countries to bring forward this type of legislation?

- Extensive and detailed consultations were necessary to ensure that the proposed legislation would strike an appropriate balance between investigative needs, industry competitiveness, and privacy.

COSTS AND COMPENSATION

What is government doing to minimize the cost to service providers?

- The legislation contains a number of mechanisms to minimize the cost to service providers.
- An initial transition period of 18 months for all telecommunications service providers is granted so as to accommodate advance planning of their network evolution and capital expenditures.
- In addition, the obligation to provide an interception capability on equipment deployed during this transition period would be deferred until the end of the 18 month transition period.
- The transition period is designed to provide service providers with time to integrate interception capability into new equipment and services.
- Clear requirements in legislation and regulations will allow the intercept requirement to be factored in during the design stage of any new technologies, avoiding today's high cost of having to retrofit solutions.
- In instances where the police and CSIS require service providers to implement interception capability within the 18 month transition period, the service providers will be compensated.
- In the area of capacity for multiple interceptions, the Government will provide compensation where this threshold must be exceeded.
- Furthermore, exemptions are available for two-year periods to permit flexibility to respond to new technologies, and to protect innovation and industry competitiveness.
- The requirements are designed to ensure specific equipment is not imposed on service providers; they will be free to select the most cost efficient solution for their particular networks based on their business practices.
- This reflects the commitment of the Government to provide a shared response to a shared problem.

Will you be compensating the telecommunications industry for implementing this legislation?

- Reasonable compensation will be provided to service providers for the specialized telecommunications support they provide the police and CSIS in implementing interceptions and providing subscriber information.

- A reasonable amount would be paid for specialized telecommunications support received by the police or CSIS for specialized technical interception assistance and for "looking up" subscriber information.

- In a situation where the 18 month transition period must be accelerated to address investigative needs, the Minister of Public Safety would provide reasonable compensation to service providers for this capability.

- The proposed legislation would set out a fee schedule in regulations. Development of these regulations is on-going.

EXAMPLES

Below are examples of requests for subscriber information. In some instances, requests were granted and helped investigations. In other instances, requests were denied and investigations were hindered.

No.	Year	Law Enforcement Agency Source	DETAILS
			Sexual Exploitation of Children
1	2007-2008	RCMP (General)	The National Child Exploitation Coordination Centre in Ottawa reported that, based on information available at the time, they were unsuccessful at obtaining subscriber information from Internet Service Providers without a court order 31.3% of the time in 2007 and 24.5% of the time in 2008. 2007 2008 Requests 482 335 - Refusal 19 (3.9%) 6 (1.8%) - No reply 92 (19.1%) 46 (13.7%) - No data available 40 (8.3%) 30 (9%)
2	2006	Toronto Police Service	Police went to the home of a 35-year-old St. Thomas man and arrested him for sexually abusing his four-year-old child live on the Internet. Fourteen months later, he pled guilty to two counts of sexual assault, three charges of making child pornography, one count of possessing child pornography and one count of distributing child pornography. The arrest of the man came only hours after he used a webcam to expose his daughter on the Internet. The sentencing judge said, "Words cannot describe what is found in those pictures." The undercover officer who was chatting with the girl's father did not know who the man was or where he lived. All he had was the man's Internet Protocol address. To find out who the man was, the officer asked the man's Internet Service Provider (ISP) for his name and address. Fortunately for this child, the ISP [immediately] provided the information and a four year old child was spared being sexually abused again.

3	2006	RCMP	An international criminal investigation involved 78 Canadian Internet Protocol (IP) addresses linked to the purchase of child pornography. Requests for subscriber information were submitted to the relevant Internet Service Providers (ISPs) and subscriber information was provided for 44 IP addresses. Cases were sent to 16 jurisdictions (multiple suspects per jurisdiction) and there were several arrests and charges for possession and accessing. 18 suspects have not been identified since the ISPs refused to provide subscriber information without a warrant. Note: Prior to the end of 2007 the National Child Exploitation Coordination Centre did not summarize all the reasons for non-cooperation.
4	2008	Ottawa Police Service	American authorities alerted the Ottawa Police Service that an internet user in its jurisdiction was trading in child pornography. In Canada, the Internet Service Provider (ISP) voluntarily gave the police the subscriber information related to the Internet Protocol address. The police then obtained a warrant to search the residence of an elderly couple for evidence that someone at their address was downloading child pornography. When police questioned the couple it became apparent they had an unsecured wireless connection and, without their knowledge, a criminal was surreptitiously using their Internet service for the purposes of exchanging child pornography online. Even though the perpetrator was not caught, the ISPs' cooperation in this investigation allowed the police to identify the address where the incident occurred and educate the residents about securing their wireless Internet access.
			Other Investigations and General Policing Duties
1	2009	Toronto Police Service	A representative of a popular children's website notified the police that a parent had posted messages threatening suicide and planning to take their child with them. Through an online "open source" search and a request for subscriber information, the police quickly identified the parent's location and intervened. They found the parent alone without that child.

2	2009	RCMP (Alberta)	Ottawa RCMP Tech Crime & Interpol notified the RCMP in Alberta of a threat made online to carry out a school shooting. Police had the Internet Protocol address and the date and time the threat was made and police requested that the Internet Service Provider (ISP) provide the corresponding subscriber information. The ISP refused to cooperate, saying there was no urgency because the threat to carry out the shooting was 6 days old. The following day (Friday before a long weekend) police applied for a production order to compel the ISP to provide the subscriber name and address information. By the time the production order was issued by a Justice of the Peace, the ISP contact had left for the weekend and the police had to wait an extra three days before obtaining the information. When the ISP complied with the production order, the police used that information to obtain an additional warrant authorizing the search of a residence. A young person was arrested and remanded pending a mental health evaluation.
3	2009	RCMP (Alberta)	An email was sent to a school, threatening to "shoot the school up at 11:00". The threat was discovered at 9:00 AM by school staff and police were called. There was a sender Internet Protocol address identified on the email, but no other data about the sender. It would have been impossible to obtain a court order to try to identify the sender and take the appropriate action to prevent the shooting in the short period of time available. Police were preparing to implement safety measures such as lockdown and police presence in the school. The Internet Service Provider agreed that exigent circumstances existed and provided the subscriber info verbally and without demanding a warrant. Police were successful in identifying and arresting the suspect at about 10:55 AM. Charges were laid against the individual.

4	2008	RCMP (British Columbia)	A person sent an anonymous email message to a University of British Columbia employee threatening to kill numerous people. Police were able to determine that the suspect used a web based email account (GMAIL) to send the death threats, but they needed the Internet Protocol (IP) address related to the email to identify the computer the suspect had used. The only way to identify the IP address in question was to get the information from the email service provider in the United States (California) because California was the only place where it was housed. The RCMP asked the Federal Bureau of Investigation (FBI) to obtain this information on its behalf from GMAIL. As requested by the FBI, GMAIL provided the IP address for the email sent on the date and time in question. The RCMP investigators then obtained assistance from a University of British Columbia Information Technology employee who, given the IP address, was able to confirm the computer used was a University of British Columbia computer located in a "common area" where students were permitted to use university computers. Police then used covert techniques for the computer in the common area and were able to identify the suspect when he returned to the same computer a few days later and sent another threat. As soon as the suspect was identified he was arrested and charged. If GMAIL in California had required the FBI to obtain a warrant before it disclosed the IP address of the University of British Columbia computer – which is what some Internet Service Providers require police to do in Canada – then the RCMP would have had to initiate a Mutual Legal Assistance Treaty (MLAT) process to have the FBI obtain a search warrant for that IP address. A MLAT process would have significantly delayed the investigation in Canada.
			Non-Criminal

1	2009	Competition Bureau	In 2009 alone, the Competition Bureau had requested subscriber information from a telecommunications service provider (TSP) for about 100 telephone numbers. The information provided has proved useful to help track down the location of various telemarketing 'boiler rooms' and has been used, along with other information, to obtain search warrants for those 'boiler rooms'. This Bill would require all TSPs, including internet service providers, to provide this type of information to Competition Bureau officers. Without this type of information being provided by the TSPs, the Competition Bureau would experience greater difficulties in identifying the individuals responsible for certain deceptive emails or websites, and therefore not be able to get search warrants or production orders to investigate them and eventually shut them down.

>>> Carole Routhier 1/20/2010 3:01 PM >>>
Good afternoon,

Should you require additional information, please do not hesitate to contact me at 613-993-1619.

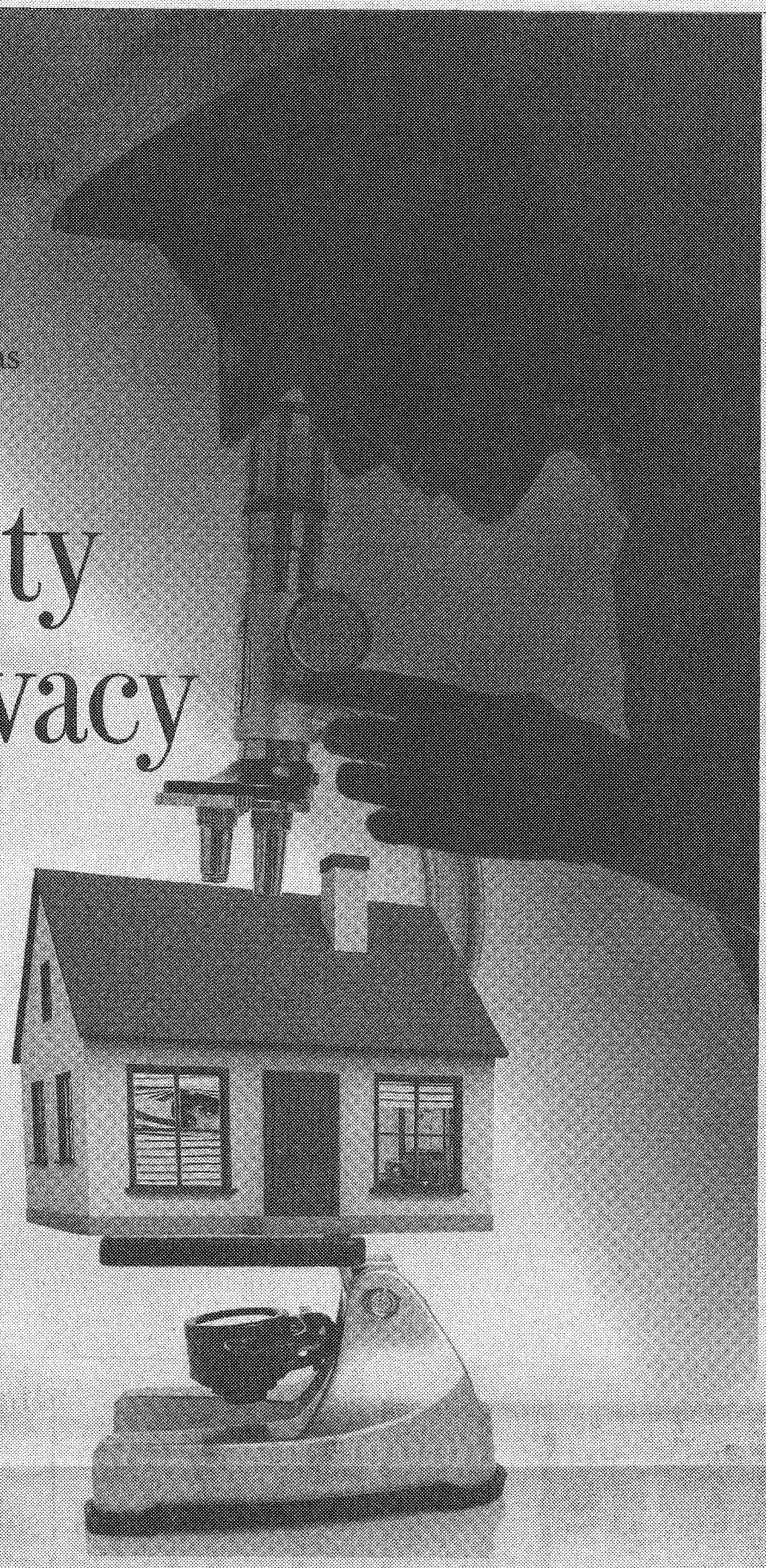
Thank you.

Carole Routhier
Administrative Assistant
RCMP Technical Operations.

CANADA

The Conservative government says 'lawful access' is a necessary tool for police in the Internet age, but as **IAN MacLEOD** discovers, its proposed legislation has revived the debate over ...

Security vs. privacy



ROBERT CROSS, THE OTTAWA CITIZEN

The "mosaic effect" is an argument often put forward by governments and police to block access to sensitive information. It suggests even seemingly innocuous pieces of information can be fitted together like a puzzle to form a meaningful picture of something they want kept secret, typically a national security operation.

But when the tables are turned and it's police and government that want to piece together seemingly innocuous bits of your personal and digital information to form a picture of you, the "mosaic effect" is recast as "lawful access" and characterized as benign state intervention into the online lives of Canadians in the name of crime-fighting.

Your name, address, telephone number, e-mail address and Internet Protocol (IP) address can reveal your Internet habits, social network, personal interests, political views, secrets and more.

The government's new "lawful access" initiative, contained in bills C-46 and C-47, was tabled in the Commons in June. It's the latest attempt in a decade-long push by successive governments to give police and other agents of the state, such as the Canadian Security Intelligence Service and the Competition Bureau, modernised surveillance powers and technical capabilities to better patrol the dark side of the digital world.

But here's the rub: C-47 allows police and government agents to demand basic subscriber data from telecommunication and Internet service providers without a warrant. (Some companies routinely volunteer the data when asked, others don't, according to police.)

In other words, police will no longer need to go before a judge and demonstrate reasonable grounds to suspect wrongdoing. They will merely have to ask companies for basic subscriber data, including in cases where they would not have had sufficient grounds to ask a court to issue a warrant.

Under former minister of public security Stockwell Day, the Conservative government pledged not to introduce mandated disclosure of subscriber data without court oversight. Yet when new Public Safety Minister Peter Van Loan and Justice Minister Rob Nicholson, flanked by more than a dozen law enforcement agents, introduced the legislation this summer, that pledge was forgotten.

Days earlier, in a letter to Prime Minister Stephen Harper, the president of the Canadian Association of Chiefs of Police had stressed that any new law requiring warrants for

What's in proposed lawful access bills

BILL C-46: Investigative Powers for the 21st Century Act

- allows enforcement agencies to require service providers to preserve all communications and data of any client named.
- creates production orders that are similar to search warrants, but require the third-party service provider to retrieve the data.

BILL C-47: Technical Assistance

ratic society."

A central issue is whether it's a reasonable and proportionate trade-off in the never-ending tug-of-war between police investigative needs and personal privacy. There can be no expectation of privacy around the commission of a criminal offence. But is that the same as saying the proposed intrusion is justified?

First, what does the evidence show?

- When Van Loan announced the proposed laws, he described a kidnapping case in which Vancouver police waited 36 hours to get the information they needed to obtain a

convince a court that a search or seizure or arrest warrant is justified.

Under the current legislation, police, for example, can't get a warrant to search or seize bank or Internet service provider records without first assuring a court that their suspect does, in fact, have an account with that business. If the business refuses to disclose basic customer data, police have to find another way. Lawful access would change that.

But, "if I want to go behind all that (basic) information, I need a warrant and that's the way it should be," says Pecknold.

Those opposed say there's a glaring contradiction in law enforcement's arguments.

"Police say, 'We really can't pursue our investigation without this critical piece of information, but by-the-by, it doesn't mean anything.' It either is the key that unlocks information that is incredibly important or, it isn't," says Micheal Vonn, of the British Columbia Civil Liberties Association.

Michael Geist, a leading Internet law expert at the University of Ottawa, agrees. "In many of these investigative situations it is going to be highly sensitive and that's precisely why law enforcement wants access to it."

Third, oversight.

The proposed legislation requires law enforcement to carry out "regular" internal audits of subscriber data requests. Any resulting concerns must be reported to the minister and copied to the applicable government watchdog, including the federal privacy commissioner, the Security Intelligence Review Committee (SIRC) that oversees CSIS, or a provincial privacy protection agency. The privacy commissioner and SIRC can also carry out compliance audits on the RCMP and Competition Bureau.

'Finding out who breaches your privacy is not to be confused with privacy protection ... You don't protect privacy after the fact.'

MICHEAL VONN
B.C. Civil Liberties Association

"We have all sorts of oversight mechanisms over the police and what they do and abuses are dealt with," says Pecknold.

Civil libertarians such as Vonn object on two fronts. "You don't protect privacy after the fact," she says. "Finding out who breaches your privacy is not to be confused with privacy protection."

And requiring law enforcement to establish "an empire of bureaucracy" to ensure the proposed measures aren't abused seems at odds with the justification that applying for warrants is too costly, time-consuming and cumbersome, she says.

"It really puts a lie to the entire rationale."

■

The U.S. experience with warrantless access is not comforting. Earlier this decade, the ultra-secret National Security Agency, by executive order, surreptitiously tapped into some of the country's major telecommunication lines, ingesting about 650 million conversations, e-mails and other communications a day from unsuspecting Americans and foreigne[illegible] whose international communica[illegible]tions were routed through the U.S.

months in June. It's the latest attempt in a decade-long push by successive governments to give police and other agents of the state, such as the Canadian Security Intelligence Service and the Competition Bureau, modernized surveillance powers and technical capabilities to better patrol the dark side of the digital world.

But here's the rub: C-47 allows police and government agents to demand basic subscriber data from telecommunication and Internet service providers without a warrant. (Some companies routinely volunteer the data when asked, others don't, according to police.)

In other words, police will no longer need to go before a judge and demonstrate reasonable grounds to suspect wrongdoing. They will merely have to ask companies for basic subscriber data, including in cases where they would not have had sufficient grounds to ask a court to issue a warrant.

Requiring a warrant for basic subscriber data 'is, in our view, harmful to public safety.'

STEVEN CHABOT
President, Canadian Association of Chiefs of Police

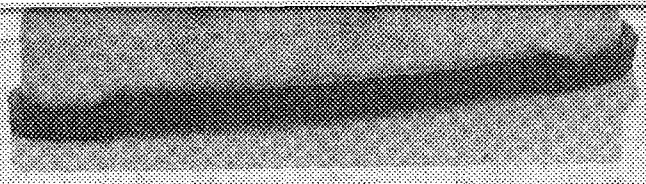
The proposed legislation stops far short of giving police total freedom to infiltrate and tap the Internet and wireless networks. Intercepting the contents of e-mails, cellphone calls and all other digital data would continue to require court approval.

Still, it's revived a sharp debate between police and their supporters and privacy and civil liberties advocates, with each camp offering hypothetical but plausible scenarios to illustrate their hopes and fears.

Consider: Armed with a search warrant, police seize a computer in a child pornography investigation. Using lawful, warrantless access, they then hunt down other suspects through their computer IP addresses and bust an international child porn ring.

Consider: Police are investigating potential security problems for the 2010 Olympics in Vancouver. Using lawful, warrantless access, they obtain from a service provider the IP addresses and identities of individuals visiting an anarchist website opposed to the Games. Police and perhaps CSIS then pay them unofficial visits to discuss their political views.

■



ROBERT CROSS, THE OTTAWA CITIZEN

Under former minister of public security Stockwell Day, the Conservative government pledged not to introduce mandated disclosure of subscriber data without court oversight. Yet when new Public Safety Minister Peter Van Loan and Justice Minister Rob Nicholson, flanked by more than a dozen law enforcement agents, introduced the legislation this summer, that pledge was forgotten.

Days earlier, in a letter to Prime Minister Stephen Harper, the president of the Canadian Association of Chiefs of Police had stressed that any new law requiring warrants for basic subscriber data "is, in our view, harmful to public safety.

"Such a requirement would impair effective and efficient criminal investigations and impose unnecessary and excessive costs on the police," wrote Steven Chabot.

Bill C-47 would also require telecommunication companies to have the technical capability for interception "backdoors" built into their networks. The rationale is that police are often operationally stymied when attempting to tap into technologies such as wireless data networks and voice over Internet protocols, creating intercept safe havens for criminals.

Key components of Bill C-46, meanwhile, allow law enforcement to serve a "preservation demand" requiring telecommunications companies and Internet service providers to "quick freeze" all communications and data of any client named in the demand. (The bill does not require companies to routinely retain customer data.)

Police would then have 21 days to convince a judge they had reasonable grounds to suspect a crime and ask for a "production order" compelling the company to disclose the information. Or, police could seek a 90-day extension to the preservation order to continue building their case for a production order.

"The objectives of justice shouldn't be defeated by advancements in technology if everybody understands and signs off on the fact that the processes that permit authorizations of the state to eavesdrop or intercept are properly governed," RCMP Assistant Commissioner Bob Paulson, head of National Security Criminal Investigations unit, said in a Citizen interview this year.

Adds Clayton Pecknold, co-chair of the law amendments committee for the chiefs' association, and deputy chief of police in Saanich, B.C.: "How are we going to master identity theft, and how are we going to combat child pornography and sexual exploitation of children and Internet luring and all of these things that are going on in the digital world if we don't have the tools that are necessary?"

■

No matter how well-intentioned, warrantless access to subscriber data is an erosion of personal privacy. There would be one less legal barrier guarding Canadians' digital fingerprints.

"It will increase powers of the police in a way that definitely impacts on privacy," says Chantal Bernier, assistant federal privacy commissioner. "What we are trying to establish is whether they can justify that intrusion in a free and democratic society."

A central issue is whether it's a reasonable and proportionate trade-off in the never-ending tug-of-war between police investigative needs and personal privacy. There can be no expectation of privacy around the commission of a criminal offence. But is that the same as saying the proposed intrusion is justified?

First, what does the evidence show?

■ When Van Loan announced the proposed laws, he described a kidnapping case in which Vancouver police waited 36 hours to get the information they needed to obtain a warrant for customer name and address information. That story, it seems, was false.

And the Criminal Code already allows police to intercept private communications in exceptional circumstances to prevent serious harm to a person or property. There's also a general consensus among service providers to voluntarily disclose information to police in "hot pursuit" cases involving child exploitation, according to the Information Technology Association of Canada.

■ Conviction rates in cases in which federal authorities have introduced intercepted evidence are remarkably low. Of 354 such cases in 2005, 13 resulted in convictions. Preliminary data for 2007 shows zero convictions out of 138 cases.

■ There were convictions in the more recent "Toronto 18" and Momin Khawaja terrorism cases, which relied heavily on Internet and e-mail evidence. But it was obtained using existing intercept and search-and-seizure laws.

■ Three senior police officers from British Columbia and Alberta who were interviewed for this story were unable to offer a single example of how the proposed legislation might have helped prevent previous real crimes.

Secondly, how sensitive and valuable is that information to individuals and police alike?

Police compare it to basic information found in phone books, tax rolls and the like. It's value, they say, is as a "building block," that helps confirm other basic pieces of information and, taken together, can help protect privacy after the fact," she says. "Finding out who breaches your privacy is not to be confused with privacy protection."

And requiring law enforcement to establish "an empire of bureaucracy" to ensure the proposed measures aren't abused seems at odds with the justification that applying for warrants is too costly, time-consuming and cumbersome, she says.

"It really puts a lie to the entire rationale."

■

The U.S. experience with warrantless access is not comforting. Earlier this decade, the ultra-secret National Security Agency, by executive order, surreptitiously tapped into some of the country's major telecommunication lines, ingesting about 650 million conversations, e-mails and other communications a day from unsuspecting Americans and foreigners whose international communications were routed through the U.S.

A review of the so-called warrantless wiretap program released in July concluded the eavesdropping resulted in no apparent counter-terrorism successes, such as arrests and thwarted plots, by the FBI, CIA and other U.S. intelligence branches.

The sophisticated "backdoor" technology used was provided by Israeli security companies, typically staffed by former Israeli military and intelligence officers and considered among the world's top manufacturers of surveillance equipment.

Representatives from two of those companies, Verint Technology Ltd. and Nice Ltd., were among several foreign security firms that gathered in Ottawa in July 2007 for an information session with senior officials from the department of Public Safety, CSIS, RCMP and the Canada Border Security Agency.

Verint, according to ministerial briefing notes obtained under access to information by Ottawa researcher Ken Rubin, discussed its "communications intercept system."

A Verint official declined to elaborate for this story. A company information sheet from the Ottawa meeting notes that Verint Communication and Interception Solutions, "capture and analyze voice and data communications, enabling government and law enforcement agencies to more rapidly identify and counter potential threats, share critical intelligence and establish evidence for legal prosecution. (It) also equip(s) telecommunications carriers to comply with government mandates on electronic surveillance."

What's in proposed lawful access bills

BILL C-46: Investigative Powers for the 21st Century Act

■ allows enforcement agencies to require service providers to preserve all communications and data of any client named.

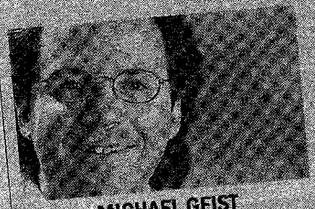
■ creates production orders that are similar to search warrants, but require the third-party service provider to retrieve the data.

BILL C-47: Technical Assistance for Law Enforcement in the 21st Century Act

■ requires telecommunication companies to have the technical capability to intercept basic subscriber information.

■ amends the Criminal Code to allow law enforcement agencies to demand basic subscriber data (names, telephone numbers, mail and e-mail addresses and Internet Protocol addresses) without first obtaining a warrant.

Internet agency should



MICHAEL GEIST

The Canadian Internet Registration Authority, the agency that administers the dot-ca domain name, holds its annual general meeting in Toronto later this week. Attendees will vie for door prizes and hear from executives about the growing number of Canadian domain name registrations, the robust financial health of the organization, and a small list of corporate bylaw amendments. Yet, as CIRA moves into its second decade, the promise of a leading Interne voice in Canada and an active, engaged membership i gradually fading away.

Engaging Canadians was viewed as a top priority d ing the organization's ear years (I was a board me from 2001-06). Meetin were held in communi across the country in fort to educate Can

2009-10-14

Jim Speedbove

- talked to Ref Soccer + CACP re: ~~Labour~~ wider conference
  ↳ Peter Cuthbert, executive director
- Proposing letter CACP, could send out with forms
- I will send examples to Rob O'Reilly + Jim Speedbove
- Jim will send me an update via Ross
- Jim suggested we simply give CACP members our internet ROSS mailbox address and they can email completed forms directly to Sp. "I" HQ.

B.T.

From: Susan Alter
To: Pownall, Tom
Date: 9/17/2009 11:37 AM
Subject: Fwd: RE: l

CC: Tremblay, Bernard

Hi Tom,
Thank you

Susan

>>> Susan Alter 9/17/2009 9:33 AM >>>
Thanks very much for this information Bernie. It is very helpful.

Susan

Susan Alter, Senior Counsel /
Avocate-conseil

RCMP Legal Services /
Services juridiques GRC
Department of Justice /
Ministère de la Justice
Ottawa, Canada K1A 0R2
susan.alter@rcmp-grc.gc.ca
Telephone /Téléphone 613-990-9090
Facsimile /Télécopieur 613-990-2343
Government of Canada / Gouvernement du Canada

>>> Bernard Tremblay 9/16/2009 5:03 PM >>>
Hello Susan,

Bernie

>>>

From: Susan Alter
To: Tremblay, Bernard
Date: 9/16/2009 9:27 AM
Subject: Fwd: RE:

CC: Bernstein, Elisa; Konarski, Tom

Hi Bernie,

Susan

From: Tom Konarski
To: Gaudreau, Mike
Date: 9/14/2009 10:44 AM
Subject: Re: Fwd: Faire suivre : Topics for Minister

CC: Bernstein, Elisa; Flynn, Mark; Tremblay, Bernard

Greetings Sir

Regards

Tom

>>> Elisa Bernstein 9/14/2009 9:46 AM >>>
email format -

thanks
Elisa

>>>
From: Mike Gaudreau
To: Bernstein, Elisa; Pasin, Sergio; Sheppard, Scott
CC:rainville, Donna
Date: 9/14/2009 9:42 AM
Subject: Fwd: Faire suivre : Topics for Minister

for your info/attention.

pls provide me with your input prior to 1000 hrs tomorrow morning.

Mike

>>> TechOps_Tasking 9/14/2009 9:37 AM >>>
Good morning,

If you do have any topics we need the info (E-mail) by tomorrow.

Mario Desjourdy
Management Services

>>> Guylaine Duperre 09/14/09 8:59 am >>>
Good morning,

The Minister's office has asked the RCMP to provide a list of possible topics for discussion for future briefings. The topics may include **issues that will require ministerial support, approval, or advance notification**. The briefings are not specific to bilats.

The final list of topics will be approved by the Commissioner and then be forwarded to Public Safety for furtherance to the Minister.

Please forward your proposed issues to my attention by **COB Tuesday September 15, 2009.** E-mail format is fine. I would suggest you include a very brief description (1 or 2 lines) of your topic if it's not self-evident. Service line leader approval is required (e-mail is sufficient). Nil replies greatly appreciated.

Should you have any questions, please do not hesitate to contact me at 993-4048.

Regards,
Guylaine

Guylaine Duperré

Acting Director, Planning and Performance Management / Directrice intérimaire, Planification et gestion du rendement
Policing Support Services / Soutien aux services de police
(613) 993-4048
Fax: (613) 949-0935

BRITISH COLUMBIA
The Best Place on Earth

NEWS RELEASE

For Immediate Release
2009AG0008-000368
September 18, 2009

Ministry of Attorney General
Ministry of Public Safety and Solicitor General

B.C. SUPPORTS CRIME-FIGHTING TECHNOLOGY AND PREVENTION

SASKATOON — British Columbia's commitment to improved federal wiretap and lawful access legislation was reaffirmed today by Attorney General Michael de Jong and Solicitor General Kash Heed, as they joined the western justice ministers' conference in Saskatoon to talk about innovative ways to both fight and prevent crime.

"We are optimistic federal changes announced earlier this year will contribute to reducing illegal gang and gun activities on B.C. streets," said de Jong. "We will continue to press Ottawa to strengthen the Criminal Code and other legislation to deter serious and violent street crime, and provide the Crown with the evidence needed to bring violent gang members to justice."

"We believe that in order to stay ahead of criminal elements, we require amended legislation that recognizes the use of new technologies such as cellphones and the Internet," de Jong said.

Another item on the agenda at the meeting was a presentation on gang prevention for parents and an overview discussion of the root causes of crime in communities, with a focus on promising approaches jurisdictions are taking.

"Here in B.C., we've done a lot of work on combating guns and gangs by emphasizing intelligence-led, integrated policing," said Heed. "At the same time, we need a balanced approach, and that means not only being tough on gang members, but being equally tough on the social conditions that breed them so we can prevent young people from joining gangs in the first place."

B.C. is urging the adoption of federal bills C-46, the Investigative Powers for the 21st Century Act, and C-47, the Technical Assistance for Law Enforcement in the 21st Century Act. The legislation would clarify the law regarding police authority to investigate criminals who are using current technologies to conduct their unlawful activities. The legislation is expected to be useful in investigations into Internet crime, cyber-stalking, child pornography, organized crime, white-collar crime and national security breaches.

The bills, introduced in the House of Commons in June, are also aimed at ensuring wireless, Internet and other telecommunications companies have the capability to intercept electronic communications and, as a result, are able to comply with court orders to provide subscriber data for criminal investigations. 277

-more-

B.C.'s ministers participated in the Sept. 18 conference using virtual technology. Both de Jong and Heed opted to attend the sessions via video conference, reducing their carbon footprint and saving the Province an estimated $5,000 in direct travel costs.

-30-

Contact: Shawn Robins
Communications Director
Ministry of Attorney General
250 387-4965

Karen Johnston
Communications Director
Ministry of Public Safety and Solicitor General
250 356-1196

For more information on government services or to subscribe to the Province's news feeds using RSS, visit the Province's website at www.gov.bc.ca.

From: Susan Alter
To: Tremblay, Bernard
Date: 9/17/2009 9:33 AM
Subject: Fwd: RE:

CC: Konarski, Tom

Thanks very much for this information Bernie. It is very helpful.

Susan

Susan Alter, Senior Counsel /
Avocate-conseil
RCMP Legal Services /
Services juridiques GRC
Department of Justice /
Ministère de la Justice
Ottawa, Canada K1A 0R2
susan.alter@rcmp-grc.gc.ca
Telephone /Téléphone 613-990-9090
Facsimile /Télécopieur 613-990-2343
Government of Canada / Gouvernement du Canada

>>> Bernard Tremblay 9/16/2009 5:03 PM >>>
Hello Susan,

Bernie

>>>

From: Susan Alter
To: Tremblay, Bernard
Date: 9/16/2009 9:27 AM
Subject: Fwd: RE:

CC: Bernstein, Elisa; Konarski, Tom

Hi Bernie,

Susan

Communications

From: Susan Alter
To: Konarski, Tom
Date: 9/16/2009 9:19 AM
Subject: Re: Fwd: online tool for reporting CNA request data

CC: Tremblay, Bernard

Tom,
FYI I am attending a meeting Friday pm with the head of Legal at Sr Deputy Sweeney's office to discuss the strategy for Lawful Access and the Privacy Commissioner's concerns.

I don't know whether Special "I" or Tech Crime (Tom Pownall) are involved in the Friday afternoon meeting; however, I think it would be very helpful if Special "I" and National Communications Services could meet before Friday afternoon to have a plan ready for the tool and for the CNA examples document release too.

Bernie ... I am going to call you to discuss this matter further.

Susan

>>> Brigitte Mineault 9/16/2009 8:14 AM >>>
Jim is back in the office tomorrow so let us know when you want us to come over. We'll bring a comms outline as a draft.

Thanks!

Brigitte Mineault
Communications Team Lead, Policing Support Services/Chef d'équipe en Communications, Soutien aux Services de Police

National Communications Services /Services Nationaux de Communication
RCMP/GRC
Tel: 613-949-0285
Cell: 613-298-9264

>>> Tom Konarski 9/15/2009 4:54 PM >>>
Hi Bernie

I haven't had a chance to set up a meeting with RCMP Comms. Could you?

Please and thanks

Tom

C-47 Communications

From: Tom Konarski
To: Mineault, Brigitte; Piche, Pierre; Tremblay, Bernard
Date: 9/14/2009 11:24 AM
Subject: Re: lawful access Op-Ed

This is an excellent rebuttal

>>> Pierre Piche 9/14/2009 11:17 AM >>>
Hi Brigitte,

Looks good from my perspective. I have included Sgt. Bernie Tremblay in the loop, so that he may review and comment as/if required.

Thanks,
Pierre

>>>
From: Brigitte Mineault
To: Konarski, Tom; Piche, Pierre
Date: 2009-09-14 11:06
Subject: lawful access Op-Ed

Tom and Pierre,

Please see below the Op-Ed the Minister's office want to send out. Any concerns with this please let me know.

Merci

Brigitte Mineault
Communications Team Lead, Policing Support Services/Chef d'équipe en Communications, Soutien aux Services de Police

National Communications Services /Services Nationaux de Communication
RCMP/GRC
Tel: 613-949-0285
Cell: 613-298-9264

>>> Liam Gerofsky 9/11/2009 4:46 PM >>>
Hi Meredith,

We don't see any immediate concerns, but are still checking with the SMEs.

Liam

-----Original Message-----
From: "Burton, Meredith" <Meredith.Burton@ps-sp.gc.ca>
To: Maureen.McGrath@ic.gc.ca<Maureen.McGrath@ic.gc.ca>
To: Butcher, Joan <JButcher@justice.gc.ca>
Cc: Savoy, Jennifer <Jennifer.Savoy@ps-sp.gc.ca>
To: Gerofsky, Liam <Liam.Gerofsky@rcmp-grc.gc.ca>
To: Spendlove, Jim <Jim.Spendlove@rcmp-grc.gc.ca>

Sent: 11/09/2009 3:16:23 PM
Subject: FYI Op-Ed

Cheers,
Meredith

Op-Ed - Bill C-47

I would like to respond to some remarks made by the Federal, Provincial and Territorial Privacy Commissioners. While I have great respect for the work they do, I feel there have been some misunderstandings about Bill C-47, the Technical Assistance to Law Enforcement in the 21st Century Act. As such, I believe clarification is needed.

First, let's start with what Bill C-47 is not: It is not about intercepting or eavesdropping on the private communications of Canadians. Nor is it about monitoring the web surfing habits of Canadians or preventing them from sending anonymous e-mails.

The proposals in Bill C-47 are about ensuring that law enforcement can keep up with new communication technologies and continue to implement warrants authorized by the courts. New technology is a powerful tool however, in the hands of criminals and terrorists, this technology can be used in ways that threaten public safety. The Government of Canada needs to update Canadian laws to keep pace with new technology - a step already taken by many of our international partners.

I want to be clear: The legislation provides no new powers to intercept communications. The existing requirements for judicial authorization for intercepts will be maintained. Since 1974, police in Canada have been authorized to intercept private communications when a court order is issued by a judge who believes on reasonable grounds that a serious offence, such as child pornography, drug trafficking, money laundering or murder, has been or will be committed. The judge must also be satisfied that authorizing the intercept is in the best interests of the administration of justice and that other investigative procedures have been tried and failed. = or are unlikely to succeed.

Nothing proposed in Bill C-47 will change these limits. Nor will it upset the strong balance established between the protection of privacy, human rights and the safety of our citizens, which are values we all cherish.

Today, telephone and Internet companies are not required to build intercept capabilities into their networks. Because of this, even with a court order, police may not be able to intercept communications. Under Bill C-47, communications providers would be required to update their systems to enable interceptions approved by the courts. To avoid undue burden, the proposed law would allow companies to build this capability gradually over time.

There have also been misunderstandings about the Government's proposals for police and CSIS to obtain subscriber information. Basic subscriber information such as a customer's name, address, telephone number and Internet address can be valuable at the initial stages of an investigation.

The problem is that while some service providers give subscriber information to law enforcement upon request, others fail to provide it in a timely fashion, or refuse to provide it at all. This has created a difference in industry practices across the country.

Access to subscriber information is particularly important in the online context, as criminals use the internet to operate with anonymity. For example, in cases where a child is lured over the internet by a sexual predator, often the only clue police have as to the identity of the perpetrator is an IP address associated with a chat room. In these situations, police need to quickly establish the identity of the suspect based on the IP address. In several cases, service providers have refused to share this information, thereby leaving some children at risk. This proposed legislation will help to ensure that there are no more dead-end investigations.

The proposed legislation would require telephone and internet companies to provide this information to designated law enforcement and CSIS officials without a warrant. Bill C-47 includes some of the very safeguards identified by the privacy commissioners to protect privacy, such as the requirement to track who is requesting the information and why, to permit audit and oversight of how the information is handled, and a five-year Parliamentary review.

Canadians can rest assured that any updates to our legislative regime will respect the privacy and human rights entrenched in laws such as the Canadian Charter of Rights and Freedoms, the Privacy Act, and the Personal Information Protection and Electronic Documents Act.

Senior advisor / Conseillère principale
Communications - Emergency Management and National Security
Sécurité nationale et gestion des urgences - Communications
Public Safety Canada / Sécurité Publique Canada

Tel: 613-949-6583
Cel: 613-219-1285
Fax: 613-993-7062
meredith.burton@ps-sp.gc.ca

NAME
NOM

IRECA - General

Parliamentary Affairs Division

Guidelines for the Legislative Process

Note: Throughout this process, the Parliamentary Affairs (PA) Division is the primary contact for the program area responsible for the Bill. PA is the main liaison with the Privy Council Office (PCO) and the Minister's Office (MO).

Preparatory Work before the Bill is Introduced

1. Preparation to brief the Minister of Public Safety (PS)

(All material must be prepared in both official languages. Often, due to time constraints, an English or French only version of each document will be accepted with the understanding that a translated version will follow shortly afterwards.)

- The Departmental/Agency senior officials brief the Minister and/or the Parliamentary Secretary once the Bill is drafted.
- The Minister's briefing book must have a common look and feel. For instance, the binder should not contain sub-sections (e.g., Section A, Subsections 1,2 and 3; Section B, Subsections 1,2,3, and 4). Please contact Parliamentary Affairs for copies of templates for the binder cover page, table of contents, and clause-by-clause analysis).
- The Minister's briefing book must, at a minimum, contain the following ***unclassified*** items:
    - Copy of the Bill
    - One page summary of the Bill (note or deck)
    - Clause-by-clause analysis – Actual clause of the Bill on the left side of the page, analysis on the right side of the page (see attachment)
    - Parliamentary Environment (produced by Parliamentary Affairs)

  The Minister's briefing book may also contain the following unclassified items:
    - Presentation deck
    - Separate notes for key elements of the Bill
    - Enhanced Qs & As
    - Other background material (comparative chart, fact sheets/briefing notes, summary of consultations, list of stakeholders)

  Please consult with PA if you feel more material should be included in the Ministerial book.

- If the bill is introduced in the House of Commons, the program area produces 12 English only copies of the briefing book for PA. PA seeks approval of the book from the Deputy Minister's Office (DMO) prior to distribution of the books to the MO. If the bill is introduced in the Senate, the program area produces 12 English only copies and three bilingual copies of the briefing binder.
- The program area must confirm the short title of the Bill with the MO Policy Advisor.

2. Preparation for Bill Review:

- Before putting a Bill on notice, PCO schedules a meeting between the Government House Leader (GHL), the sponsoring Minister(s) and a government official (subject matter authority). PA notifies the Department and the agencies of the logistics of the meeting.
- Ideally, the Ministerial briefing binder serves to brief the Minister at all stages - whether it be for his actual briefing on a bill, or for his meeting with the Government House Leader (or Bill Review meeting). Should the Ministerial binder not be complete in time for the Bill Review, the Minister's Office has requested at least the following documents be provided:
    - Copy of the Bill (latest draft if not finalized)
    - Explanatory note or deck
    - Parliamentary Environment (produced by PA)

- The Minister can be accompanied by only one government official - usually a subject matter authority.

3. Preparation of Speeches for Use in the House of Commons (or Senate) at Second Reading:

- The speaking material is prepared by the Speechwriting Unit in the Communications Directorate in consultation with the program area.
- Normally, a total of three speeches (varying from 10 – 20 minutes in length) are required for use by the Minister, the Parliamentary Secretary, and a Government M.P. during the debate. PA tasks the Speechwriting Unit.
- The speeches must be provided to PA in both official languages.
- The speeches can be adjusted to reflect last minute changes if necessary just before Second Reading.

4. Preparation of Information Packages for Opposition MPs (if necessary)

- The MO may wish to provide briefing sessions to Opposition critics once the Bill is introduced.
- A bilingual information package (or kits) for Members is prepared by the program area and must contain the following:
    - Copy of the Bill
    - One page summary of Bill
    - Basic, explanatory Q & As

  The information package may also contain some or all of the following items:
    - Explanatory Deck (factual information in the public domain)
    - Separate notes for key elements of the Bill (where applicable)

- The number of copies of the package is to be confirmed by PA. PA seeks approval of the DMO and the MO prior to the briefing.
- All materials provided must be unclassified and must not contain Cabinet confidences.

5. Introduction of the Bill (First Reading)

- The GHL is responsible for determining when a government Bill is to be introduced. PCO informs PA, who will in turn, inform the program area.
- Forty-eight hours notice is required for introduction in the House (handled by PCO). No notice is required for Bills introduced in the Senate.
- The program area must provide 60 copies of the Bill to PA at least 48 hours before introduction as well as a pdf. version of the Bill.
- Once introduced, the Bill is printed and given a number by House officials. There is no debate in the House (or Senate) at Introduction.
- Communications Directorate prepares a news release, backgrounder, and other related communications products.
- No officials are required in the government lobby of the House to assist the Minister for Introduction.

Material to be Produced once the Bill is before the House or Senate

6. Preparation of Information Material for a Parliamentary Committee

- The committee members will be provided with a bilingual, scaled down unclassified version of the Minister's briefing book.
- The program area produces 25 bilingual copies of the information book for PA which seeks approval of the DMO and the MO prior to delivering the books to the Committee.
- The information book for all committee members must be prepared by the program area and must contain the following three items contained in the Minister's book:
    - Copy of the Bill
    - One page summary of the Bill
    - Clause-by-clause analysis

  Please consult with PA if you feel more material should be included as part of the Committee book.

- All materials contained in the Committee book must be unclassified. All Committee binders must be in bilingual format (English and French versions of the same document separated by a coloured piece of paper and placed under the same tab).
- PA is responsible for distributing the books to the Committee, the Minister's Office, and Deputy Minister's Office. We require 25 bilingual books for the House of Commons Committee (or Senate Committee if a bill is introduced in the Senate). Later in the process, we will require additional 25 bilingual copies of the book for the Senate Committee (or the House Committee if a bill was introduced in the Senate).
- In addition, the Minister's Office requests three additional Committee binders before a bill is introduced in the Senate for distribution to Senators.

7. Preparation for an Appearance by the Minister before a Parliamentary Standing Committee (House and Senate)

(Before the Bill is referred to Committee)

- If required, the Minister's briefing book is updated and 12 copies are assembled by the responsible Branch.
- The following updates may be required for the Minister's book – (see Section 1):
  - Any new Ministerial correspondence related to the issue
  - Updated Media lines
  - Summary of Second Reading debate and Q & As to address concerns raised during the debate
- The Minister's opening statement before Committee (10 minutes, in both official languages) is prepared by the Speechwriting Unit in consultation with the program. PA tasks the Speechwriting Unit.

8. Debate at Second Reading:

- The timing for Second Reading debate is determined by the GHL. PA informs the Department/Agency.
- Updates to the speeches and talking points to ensure currency can be made as required before the debate begins.
- The program area is encouraged to monitor the debate – with particular attention to opposition party concerns. The Speechwriting Unit keeps track of speeches read into the record and, if necessary, to update any "unused" speeches to reflect any concerns raised by opposition members.
- Officials must be prepared to be in the Government Lobby of the House of Commons. PA will coordinate the participation of officials with DMO and MO in the event MO requires the presence of a subject matter authority.
- Additional speeches may be required should the debate continue for a prolonged period of time. PA tasks the Speechwriting Unit.

9. Committee Stage:

- The Minister will likely be invited to appear before Committee and will require a 10 minute opening statement in both official languages (prepared by the Speechwriting Unit in consultation with the program area).
- An updated briefing book may be provided to the Minister (See Section 7).
- The Committee may call a number of witnesses and schedule many meetings to study the Bill.
- The Committee will proceed with clause-by-clause analysis of the Bill at the very end of the Committee Stage.
- The Committee will "report" the Bill (with or without amendments) to the House.
- Officials need to be available to appear before committee including during the clause-by-clause consideration of the Bill.
- PA may occasionally request additional material not outlined in this document.

Amendments to a Bill at Committee (during the Clause-by-Clause Meeting)

- Officials may be asked to provide a detailed analysis of proposed opposition amendments and possible impacts on very short notice – sometimes moments after the amendment has been moved at Committee.

Steps for the program area to follow for Opposition Amendments:

(in the event the text of the amendment is provided in advance of the Committee meeting)

- Draft a note to the Minister that includes: i) the actual text of the amendment; ii) the impact of the amendment; and iii) at least two talking points

Steps for the program area to follow for Government Amendments:

- Contact PA as soon as Department/Agency officials identify a need to further amend the Bill.
- Engage the MO and draft a memo to the Minister providing a rationale for the amendment(s).
- Engage your PCO policy analyst to assess whether the amendment will require Cabinet approval. At the same time, engage your Legal Affairs contact at the Department of Justice (DOJ) to ensure the amendment is within the scope of the Bill. DOJ will ultimately draft the amendment.
- Should the Minister not have policy coverage, it is possible that a Memorandum to Cabinet or a letter to a Cabinet committee will have to be drafted by the program area.
- Draft a note for use by the Parliamentary Secretary that includes: i) the actual text of the amendment; ii) a rationale for the amendment; and iii) at least two talking points

- PA will liaise with our PCO counterparts at Legislative and House Planning (L&HP) and the MO (Director of PA) with respect to the procedural considerations for moving the amendment(s) at Committee.

- PA can provide an example of a motion to amend a Bill at Committee.

10. Report Stage

- The Bill can be further amended at this stage.
- The MO will provide instructions as to the number of speeches and what each speech should address. PA tasks the Speechwriting Unit.
- Officials must be prepared to produce speeches and/or talking points as well as detailed analysis of any opposition amendments on very short notice.
- For details on steps to follow for opposition amendments, please see section 9 – amendments at Committee Stage.
- PA will inform the program area of any amendments put on notice.

11. Third Reading

- The requirements for speeches will become more apparent as the Bill works its way through the legislative process. Usually two speeches (10 minutes), in both official languages, are required. PA tasks the Speechwriting Unit.

12. Preparation for the Briefing of Sponsoring Senator

- The briefing material produced for the Committee study would likely suffice - See Section 6. Briefing materials for use by the sponsoring Senator must always be in both official languages. A total of three briefing books is required for the sponsoring Senator.

13. Senate Process

- Essentially the same processes are repeated in the Senate (i.e., three readings, committee, and report stage). Bills can be amended at any stage in the Senate.
- Note: If the bill is introduced in the Senate, the program area produces 12 English only copies and three bilingual copies of the briefing binder.

14. Royal Assent

- No material is required from the Department/Agency
- Usually, the Senate waits until there are a number of Bills that are ready for Royal Assent before a ceremony takes place. Often, Royal Assent is signified by a written declaration by the Governor General or a Justice of the Supreme Court acting on his behalf.
- Once the Bill receives Royal Assent, it is assigned a chapter number. These chapters are assigned chronologically according to Royal Assent date and are published in the *Canada Gazette, Part III.*

15. Coming into Force (Proclamation)

- Normally, the date of Royal Assent is the date the Act comes into force, but the Act may provide for the date(s) to be fixed by an Order in Council.
- The Coming into Force clause is normally found at the end of the Act. It may state that the provisions of the Act come into force: i) on a day to be fixed by an order of the Governor in Council; ii) on a specified date; or iii) in specified circumstances. Different provisions of the Act may come into force on different dates. If the Bill does not include a coming into force clause, the Bill comes into force on the day it receives Royal Assent.
- The Department/Agency is responsible for preparing a submission for the Minister's signature requesting the issuance of a proclamation through a submission to the Governor in Council for an Order in Council authorizing the proclamation to be issued.
- PA does not play a role with respect to the Coming into Force provisions of a Bill. If the Bill is to come into force by an order of the Governor in Council, please contact your Treasury Board Secretariat analyst within the Cabinet Committee Operations, Regulatory Affairs Section to learn of the appropriate process, or call 613-943-5076 or e-mail info@tbs-sct.gc.ca for assistance.

From: Tom Pownall
To: Bernstein, Elisa; Konarski, Tom
CC: Gaudreau, Mike
Date: 9/23/2009 3:29 PM
Subject: Fwd: Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials on Bills C-46 and C-47

as discussed

>>> <bmunson@itac.ca> 9/10/2009 10:07 AM >>>
ITAC Cyber Security Forum, Legal Affairs Forum and Lawful Access Task Force

Thanks to Joel Thorp at Rogers, here's a noteworthy news release, which can be found online at: http://www.priv.gc.ca/media/nr-c/2009/res_090910_e.cfm

Bill Munson
ITAC

****

"Protecting Privacy for Canadians in the 21st Century"
Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials on Bills C-46 and C-47
September 9-10, 2009, St. John's, Newfoundland and Labrador

CONTEXT

1. The federal government tabled two pieces of legislation in June 2009 aimed at giving Canadian law enforcement, national security agencies and others (hereafter referred to as "authorities") broader powers to acquire digital evidence to support their investigations.

2. Bill C-46, the Investigative Powers for the 21st Century Act (IP21C), would allow authorities to order telecommunications providers to preserve and turn over the details of their subscribers' communications. Authorities would also have the power to apply for special orders to trace mobile communications devices and, by extension, their owners.

3. Bill C-47, the Technical Assistance for Law Enforcement in the 21st Century Act (TALEA), would give authorities access to information about subscribers and their mobile devices, even without a warrant. The bill would also oblige all telecommunications companies to build in a capability allowing authorities to intercept communications on their networks.

4. The provisions of the proposed Acts raise privacy concerns. For instance, without a warrant, authorities could gain access to personal information such as unlisted telephone numbers, and e-mail and IP addresses.

5. Canadians consider much of this personal information to be sensitive and expect it to be kept confidential.

6. Canadians also expect their use of computers and mobile devices to remain private.

7. The legislation as currently drafted is not limited only to investigations of serious criminal offences, but also could be used to target even minor infractions and non-criminal matters.

WHEREAS

1. Privacy is a fundamental human right that enables the freedom of association, thought and expression.

2. Canadian courts have consistently affirmed the importance of these rights.

3. Canada has a legal regime governing the use of surveillance that protects individual rights while also giving authorities access to communications when authorized. This framework has been carefully refined over decades by Parliament and the courts.

4. To date, the federal government has presented no compelling evidence that new powers are needed.

THEREFORE

The Federal, Provincial and Territorial Privacy Commissioners of Canada urge Parliament to ensure that the proposed legislation to create an expanded surveillance regime strikes the right balance between individual privacy and the legitimate needs of the authorities by:

1. Approaching IP21C and TALEA with caution because they alter a carefully constructed and workable framework;

2. Obliging the government to demonstrate that the expanded surveillance powers they contain are essential and that each of the new investigative powers is justified;

3. Exploring the alternative that, should these powers be granted, they be limited to dealing with specific, serious crimes and life-threatening emergencies;

4. Ensuring that any legislative proposals on surveillance:
   a. Be minimally intrusive;
   b. Impose limits on the use of new powers and ensure appropriate legal thresholds remain in place for court authorization;
   c. Require that draft regulations be reviewed publicly before coming into force;
   d. Include effective oversight;
   e. Provide for regular public reporting on the use of powers; and
   f. Include a five-year Parliamentary review.

Presentation to Privacy Commissioner
July 9, 2009

RCMP
ROYAL CANADIAN MOUNTED POLICE

Lawful Access and Policing

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

RCMP
ROYAL CANADIAN MOUNTED POLICE

Background

Lawful access consists of legislative measures:

- ✓ **for lawful interception infrastructure obligations; and**
- ✓ **for customer name and address (CNA) information.**

- **Such measures are essential in the prevention, investigation and prosecution of serious offences, including organized crime, and threats to national security.**
- **Such measures are subject to and respect the *Canadian Charter of Rights and Freedoms***

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Background

- Lawful Access measures are an essential component of the Government's Public Safety Agenda, National Security Policy and Anti-Terrorism Plan, as well as the Speech from the Throne commitments to combat child pornography and hate crimes.
- Canada and Japan are the only G-8 countries that do not have intercept capability legislation.
- New legislation requiring telecommunications service providers (TSPs) to develop and maintain intercept capable systems would not grant new surveillance powers to police or national security agencies.
- Police and national security agencies derive their lawful authority to intercept communications (e.g. wire tap) from other federal laws.

RCMP
ROYAL CANADIAN MOUNTED POLICE

Lawful Interception Infrastructure Obligations

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

The Need for Legislated Infrastructure Obligations

- Rapidly improving telecommunications technologies clearly benefit Canadian society in many ways, but their illicit use creates significant public safety challenges.

- Technologies such as the Internet, cellular telephones, smart phones and encryption increasingly challenge law enforcement and national security agencies' lawful interception capabilities.

- Criminals and terrorists are using these technologies to shield their activities from detection and as tools to facilitate the commission of serious offenses.

RCMP
ROYAL CANADIAN MOUNTED POLICE

The Need for Legislated Infrastructure Obligations

- Since the mid-1990s, deregulation, technological evolution, and user demand of the telecommunications industry has led to the creation of over 400 TSPs in Canada and new telecom services, such as VoIP (voice over IP) services.
- The telecommunications environment, in which law enforcement and national security agencies must carry out their investigations, now is constantly in flux.
- Federal laws allow courts to authorize law enforcement and national security agencies to intercept communications, but there are no laws in Canada that require telecommunications service providers to develop and maintain systems capable of being intercepted.
- As a result, law enforcement and national security agencies are spending considerable time and money developing technical solutions.
- Also, investigations of serious crimes are delayed and public safety is compromised.

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

RCMP
ROYAL CANADIAN MOUNTED POLICE

Customer Name and Address (CNA) Information

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Problem with the Status Quo is Reliance on Voluntary Cooperation

- Requests for voluntary release of customer name and address information are currently made:
  - Formally – e.g., by Law Enforcement Request (LER) forms that police and certain ISPs have agreed to use for child sexual exploitation cases
  - Informally – e.g. by verbal or written request to a TSP for any other law enforcement purpose (general policing or investigative duties)
- RCMP's National Child Exploitation Coordination Centre maintains data on LER requests, but for all the other types of investigation we do not do so
- Other police services don't keep a running total or other data about informal requests to TSPs for voluntary disclosure of CNA
- Statutory requirements for requesting and protecting CNA would clarify for TSPs and law enforcement agencies what Parliament and the public expects of them

RCMP
ROYAL CANADIAN MOUNTED POLICE

Need For Legislative Access to TSPs' CNA Info

- Police require CNA for their daily work. Police need to receive CNA on request (without a warrant process) for:
  - General policing duties (e.g., locating people in crisis, such as suicidal people, and finding and notifying next of kin)
  - Greater efficiency & effectiveness (i.e., CNA is preliminary information, gathered at the early stages of an investigation (pre-warrant) and if that investigation matures then police would use the CNA in applying for a warrant or other court order to collect evidence. It is inefficient and ineffective to require CNA through a warrant process at a preliminary stage).
  - Fast moving, time sensitive investigations (e.g., abductions and child abuse) where there is no time to get a warrant

RCMP
ROYAL CANADIAN MOUNTED POLICE

Should law enforcement have warrantless access to CNA information?

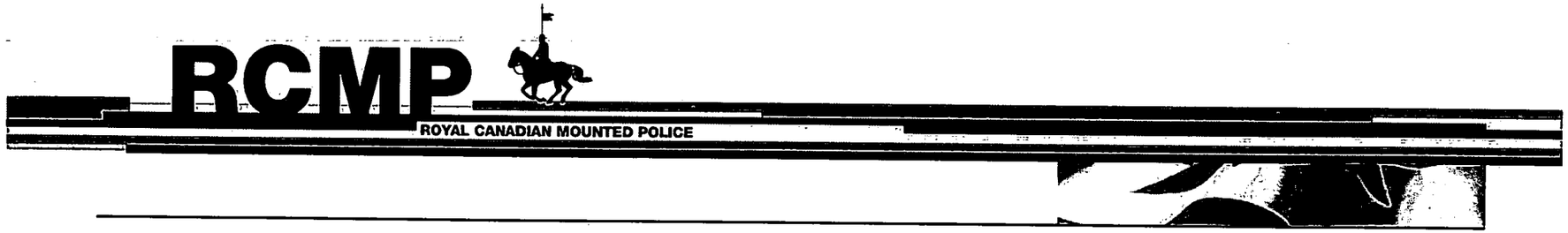
- Obtaining warrants in the early stages of a criminal investigation may not be possible as police simply might not yet have gathered sufficient information to meet the grounds necessary to be able to apply for a warrant.

- Obtaining warrants for general policing duties is not possible because no criminal offence is under investigation hence obtaining a warrant is not an option.

- For either purpose, investigative or to perform general policing duties, it is the position of the police that obtaining a warrant for basic customer identifying information such as CNA information is not required by the law.

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada



Concerns About Warrants for CNA

- Obtaining timely CNA information with a warrant in fast-moving or time sensitive investigations such as multi-million dollar Internet frauds, sexual assaults or other serious crimes in progress is not practical.
- The time spent by police to prepare and the courts to process warrant applications for CNA is not an effective or efficient use of limited criminal justice resources.
- If a new warrant was created for police to obtain CNA from TSPs, then all the police requests that TSPs are voluntarily meeting right now would have to be processed as warrants potentially leading to additional strains on the courts.
- Police do not know across Canada, in all jurisdictions, how many CNA requests TSPs are answering voluntarily each year. However, RCMP does know that in 2008-09, three of Canada's estimated 400 TSPs processed 600+ CNA requests for RCMP NCECC.

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

The Gap Between the Law and Voluntary Release of CNA

- Section 8 of the Charter protects information that attracts a "reasonable expectation of privacy".
- The Supreme Court of Canada has affirmed in a number of cases, such as *Plant,* that a person's non-core biographical information does not attract a reasonable expectation of privacy.
- As of 2008, a body of case law has emerged in the lower courts expressly considering whether police can seek voluntary disclosure from an ISP of a customer's name and address only, for the purposes of a child pornography investigation, by making a request without a warrant and whether or not there is a reasonable expectation of privacy in that information.

The Gap Between the Law and Voluntary Release of CNA

- In January 2008, an Ontario lower court ruled in *Kwok* that police should have obtained a warrant for the release of CNA information from an ISP for a child pornography investigation.

- Since *Kwok*, there have been at least nine other lower court rulings in Ontario and one in Saskatchewan that found police investigating child pornography could lawfully obtain CNA information from Internet Service Providers (ISPs) without a warrant.

- In spite of these rulings companies in the Atlantic region, such as Aliant and Eastlink, steadfastly continue to refuse to provide CNA in child pornography cases unless police serve them with a warrant to release that information.

RCMP
ROYAL CANADIAN MOUNTED POLICE

Lawful Access – Operational Impact

- The absence of Lawful Access legislation impacts every aspect of policing.
- Real life examples: sexual exploitation of children, organized crime and terrorism.

Conclusion

- **It is essential in the prevention, investigation and prosecution of child sexual exploitation, organized crime, threats to national security, and other serious offences that:**
  - **Police have legislated warrantless access to customer name and address information; and**
  - **Telecommunication Service Providers are required to develop and maintain intercept capable systems.**

Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

scan

Customer Name and Address (CNA) Information Consultation Document

Response of the Office of the Privacy Commissioner of Canada to Public Safety Canada

October 2007
Ottawa, Ontario

Jennifer Stoddart
Privacy Commissioner of Canada

?

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.

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,

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

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);
- 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.

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

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.

Section 8 of the Charter of Rights and Freedoms protects Canadian against unreasonable search and seizure when there is a reasonable expectation of privacy.

---

[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.

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.

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

---

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

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.

CUSTOMER NAME AND ADDRESS 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.

2. Police are not requesting personal information that is confidential or sensitive

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. But some IPS refused to cooperate. 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.

In September 2007, RCMP Special "I " assisted Toronto Police Service (TPS) with a Mutual Legal Assistance Treaty (MLAT) request received from the Federal Bureau of Investigation (FBI). The objective of this operational request was to identify the individual who was accessing unsecured wireless computer networks in Canada ("war driving") in order to use other people's Internet access points to commit fraudulent activities against large U.S. corporations.

The suspect was constantly moving around the Toronto area to avoid detection. The FBI could detect when unauthorized connections were made to the victims' unsecured wireless networks and the IP address of the unsecured access point where the suspect would log onto the Internet. It was the responsibility of the RCMP to respond to reports from the FBI of unlawful network access in an effort to track down the location of the suspects. To do so, in real time, the immediate support of ISPs was needed.

Once the FBI provided the IP address of the access point, RCMP could determine who the Internet Service Provider (ISP) was as certain blocks of IP addresses are issued to certain ISPs. This ISP information is openly available on the Internet. The ISP would subsequently be contacted and if they co-operated, they would give police the civic address. Police would then proceed to the area in an attempt to locate the suspect who would be operating within a quarter kilometer of the physical address of the access point.

However, without a warrant or court order, in this case the ISPs would not provide the customer name and address information to police. The most detailed information one ISP gave police was that the IP address was located somewhere on Yonge Street, which is a street that stretches from Lake Ontario to the city of Barrie.

Because of the lack of cooperation from ISPs it took eight full-time technical investigators five days to finally locate and arrest the suspects. The suspects' attempted frauds were valued at $100 million. They were successful at actually defrauding victims of $15 million.

The very fast moving nature of this investigation precluded investigators from obtaining warrants or court orders for the numerous IP addresses that were being provided "live" by the FBI to Canadian investigators.

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 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

[5] S.C. 2000, c. 5, ss. 11 to 17.

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>

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 Diego, California; Wolak, Janis, Finkelhor, David, and Mitchell, Kimberly J. (2005). "Child-pornography

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 including but not limited to database checks, CPIC, and physical surveillance of the residence. Once sufficient evidence exists, a search warrant for the residence

---

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

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.

PART TWO:
THE ADMINISTRATIVE MODEL AS A REASONABLE SOLUTION

The RCMP believes that in Canada, a reasonable, balanced, effective, well-regulated and accountable solution is needed for police to obtain basic customer identifying information to protect the public interest in safety, security and the suppression of crime while safeguarding individual privacy interests. In the RCMP's view this objective could be accomplished by the proposals for legislation that would establish the administrative model and build in solid, privacy-related safeguards. If one looks to the American example, one will find their Administrative Subpoena, which is issued by police, to be a similar type of administrative solution for obtaining this type of information.

The RCMP notes that in past consultations some participants have commented on the lack of publicly available information describing what a legislated administrative model could achieve. While Public Safety Canada's consultation document outlines that an administrative model is under consideration and summarizes general safeguards that could be incorporated in legislation, it does not provide a detailed picture of what a possible legislated framework could feature.

On the other hand, the RCMP notes that some detailed examples are publicly available online and they offer a clear picture of what such a model could entail. In Canada legislative proposals have been developed and tabled in the House of Commons as Bill C-74 in November 2005 and revived and re-packaged as a Private Member's Bill (Bill C-416), which received first reading in March 2007.

Therefore, in this part of the submission, the RCMP will be referring to provisions in these bills simply because, to date, they offer the most detailed examples to be found in the public domain that illustrate in concrete form what a legislated administrative model could encompass. By referring to actual provisions found in proposed legislation, the RCMP can explain more fully how, in its view, a legislated administrative model could provide a reasonable, balanced, and effective solution to the "CNA problem", within a well-regulated and accountable system.

By commenting on specific legislative proposals that now exist in the public domain, our purpose is not to champion any particular bills. What legislation would be most suitable and would be supported by Canadians is political matter for elected law-makers to determine. Rather reference to certain provisions in these bills will be made to highlight in a concrete (less theoretical and more practical) way how legislation could be used to resolve the CNA issue, meet important public policy objectives, and balance public interests at the same time.

3. Advantages of the legislative model

Although such a legislated administrative model would not involve police in seeking a warrant or a court order for the information in question, a reasonable and accountable process for lawfully obtaining this information could be established, regulated and administered under federal legislation. It is important to emphasize that a legislated regime for police to obtain certain customer information without having to obtain the prior approval of a court official does not mean police would have unbridled access to the information in question. It does mean that police requests for customer identifying information would be well-regulated and that Parliament could ensure privacy interests, as well as other public interests, would be fostered using this model.

Furthermore, the legislation would impose a clear legal requirement on telecommunications service providers to provide certain customer information to police when it is requested pursuant to the legislation. Such a requirement should satisfy the companies' liability concerns and eliminate the problems police face with service providers who currently choose not to cooperate with police.

The checks and balances would be in statute rather than falling to the courts to administer through the oversight they exercise in considering warrant applications. However, the authority for police to obtain the information and the controls over the request process would be entrenched in law with appropriate oversight and accountability built into the legislation.

Furthermore, since this legislative model would not require police to make applications to a court official (such as a Justice of the Peace) but rather would require police to submit

written requests for the information to service providers, this process would not place new demands on an already over-burdened court system.

CONCLUDING REMARKS

The RCMP is satisfied that if Parliament were to legislate an administrative model to govern police requests to obtain identifying information for telephone and ISP customers, the type and amount of protection provided through such legislation would be reasonable and would meet public policy objectives while being proportional with the level of privacy that the public expects lawmakers to give this type of basic (non-intimate) customer identifying information.

The RCMP does not believe the same objectives could be accomplished as effectively through some type of new warrant that could be created in legislation.

The RCMP is grateful for having been given the opportunity to express its views on the issues associated with police seeking reasonable, lawful and effective access to customer identifying information.

Review
Translation

From: Daniel Lacroix
To: Piche, Pierre
Date: 9/2/2009 11:09 AM
Subject: CNA Reporting Template
Attachments: LER - CNA Requests - Individual Report.doc; LER - CNA Requests - Multiple Report.doc

CC: Dodier, Amanda

Bonjour Pierre,

Voici tel que promis la traduction des formulaires. Si tu as des questions, tu peux m'appeler.

Daniel

Daniel Lacroix
Intelligence Analyst / Analyste de renseignements
National Child Exploitation Coordination Centre (NCECC)
Centre national de coordination contre l'exploitation des enfants (CNCEE)
890 Taylor Creek
Orleans, Ontario
K1A 0R2
Office: (613) 841-3522
Fax: (613) 949-0820
E-mail / Courriel: daniel.lacroix@rcmp-grc.gc.ca

Sous-direction des services d'enquêtes techniques
Rapport individuel : Demande relative aux nom et adresse d'un abonné

But du rapport:

Compiler des données sur les demandes que soumettent aux fournisseurs de services de télécommunication (FST) les services de police canadiens relativement à la divulgation volontaire du *nom* et de l'*adresse* d'un de leurs abonnés. La GRC compile ces données au nom de l'ensemble de la communauté policière. Les noms et les adresses ne sont toutefois pas compilées dans le cadre de ce rapport.

Notes relatives au rapport:

1) Ce formulaire ne doit être rempli que lorsqu'un service de police demande à obtenir le nom et l'adresse d'un seul abonné.
2) Ce formulaire ne porte que sur les demandes relatives aux noms et aux adresses. Il ne doit pas être utilisé lorsque la demande vise à obtenir d'autres informations sur l'abonné.
3) Ce formulaire doit être utilisé que lorsqu'un service de police demande à un FST de divulguer volontairement de l'information, et non lorsque la demande fait suite à une ordonnance de la cour.
4) Ne pas remplir ce formulaire si le Centre national de coordination contre l'exploitation des enfants (CNCEE) a déjà soumis une demande d'application de la loi (LER) au FST.
5) Ce formulaire doit être envoyés dans les cinq (5) jours ouvrables suivant la soumission de la demande au FST. Aux fins du rapport, on considèrera que le FST n'a pas répondu à la demande si la réponse n'a pas été reçue dans les cinq (5) jours ouvrables suivant sa soumission.

Service de police :

Province/Territoire :

Q1 : À quel type de FST votre demande a-t-elle été envoyée?

Q2 : Dans quel but demandiez-vous le nom et l'adresse de l'abonné?

Q3 : Si la demande s'inscrivait dans le cadre d'une enquête criminelle, de quel type d'infraction s'agissait-il?

Q4 : Le FST a-t-il répondu à la demande?

Q5 : Si le FTS n'a pas fourni les nom et adresse de l'abonné, quelle a été la raison invoquée?

Q6 : Lorsque vous avez soumis la demande au FST dans le cadre d'une enquête sur une infraction, disposiez-vous à votre avis de motifs suffisants pour demander une ordonnance de la cour?

Q7 : Si le FST n'a pas fourni les nom et adresse de l'abonné, quels ont été les répercussions sur l'enquête ou sur les fins auxquelles la demande avait été soumises?

Indiquer la date à laquelle la demande visée par ce rapport a été soumise :

Date Mois Jour

Imprimer

Effacer

Envoyer par courriel

Merci de bien vouloir remplir ce formulaire. Pour nous l'envoyer, veuillez cliquer sur le bouton «Envoyer par courriel».

Sous-direction des services d'enquêtes techniques
Rapport multiple : Demande relative aux nom et adresse d'un abonné

But du rapport :

Compiler des données sur les demandes que soumettent aux fournisseurs de services de télécommunication (FST) les services de police canadiens relativement à la divulgation volontaire du *nom* et de l'*adresse* d'un certain nombre de leurs abonnés simultanément. La GRC compile ces données au nom de l'ensemble de la communauté policière. Les noms et les adresses ne sont toutefois pas compilées dans le cadre de ce rapport.

Notes relatives au rapport:

1) Ce formulaire ne doit être rempli que lorsqu'un service de police soumet une demande à un FST pour obtenir le nom et l'adresse de plus d'un abonnné (multiples abonnés) dans le cadre d'une enquête, d'une opération ou d'un dossier.
2) Ce formulaire ne porte que sur les demandes relatives aux noms et aux adresses. Il ne doit pas être utilisé lorsque la demande vise à obtenir d'autres informations sur les abonnés.
3) Ce formulaire ne doit être utilisé que lorsqu'un service de police demande à un FST de divulguer volontairement de l'information, et non lorsque la demande fait suite à une ordonnance de la cour.
4) Ne pas remplir ce formulaire si le Centre national de coordination contre l'exploitation des enfants (CNCEE) a déjà soumis une demande d'application de la loi (LER) au FST.
5) Pour chaque question, on peut cocher plus d'une case s'il y a lieu.
6) Ce formulaire doit être envoyés dans les cinq (5) jours ouvrables suivant la soumission de la demande au FST. Aux fins du rapport, on considèrera que le FST n'a pas répondu à la demande si la réponse n'a pas été reçue dans les cinq (5) jours ouvrables suivant sa soumission.

Service de police :

Province/Territoire :

Q1 : À quel type de FST votre demande a-t-elle été envoyée?
- Fournisseur d'accès internet
- Compagnie de téléphone
- Autre (p. ex. : site de réseautage social)

Q2 : Dans quel but demandiez-vous le nom et l'adresse des abonnés?
- Enquête sur une infraction criminelle
- Enquête sur un autre type d'infraction
- Police générale (non reliée aux enquêtes)
- Renseignement criminel

Q3 : Si la demande s'inscrivait dans le cadre d'une enquête criminelle, de quel type d'infraction s'agissait-il?

Exploitation sexuelle d'un enfant
Drogue et crime organisé
Fraude et crime financier
Enlèvement, personne disparue
Homicide
Autre
Sans objet (l'enquête ne portait pas sur une infraction criminelle)

Q4 : Le FST a-t-il répondu à la demande?

Information fournie
Information partielle fournie
Information non fournie

Q5 : Si le FTS n'a pas fourni les nom et adresse de l'abonné, quelle a été la raison invoquée?

Le FST exige une ordonnance de la cour
Le FST n'a plus les donnée demandées ou n'en a plus le contrôle
Aucune raison fournie
Autre
Sans objet (les données demandées ont été fournies)

Q6 : Lorsque vous avez soumis la demande au FST dans le cadre d'une enquête sur une infraction, disposiez-vous à votre avis de motifs suffisants pour demander une ordonnance de la cour?

Oui
Non
Difficile à dire, car les motifs n'étaient pas les mêmes pour chaque abonné
Sans objet (p. ex. : la demande n'a pas été faite à des fins d'enquête)

Q7 : Si le FST n'a pas fourni les nom et adresse de l'abonné, quels ont été les répercussions sur l'enquête ou sur les fins auxquelles la demande avait été soumises?

Il a fallu mettre fin à l'enquête ou à l'opération ou clore le dossier
Il a fallu retarder l'enquête, l'opération ou le dossier
L'enquête, l'opération ou le dossier ont pu continuer, mais partiellement
Sans objet (les données demandées ont été fournies)

Indiquer la date à laquelle la demande multiple visée par ce rapport a été soumise :

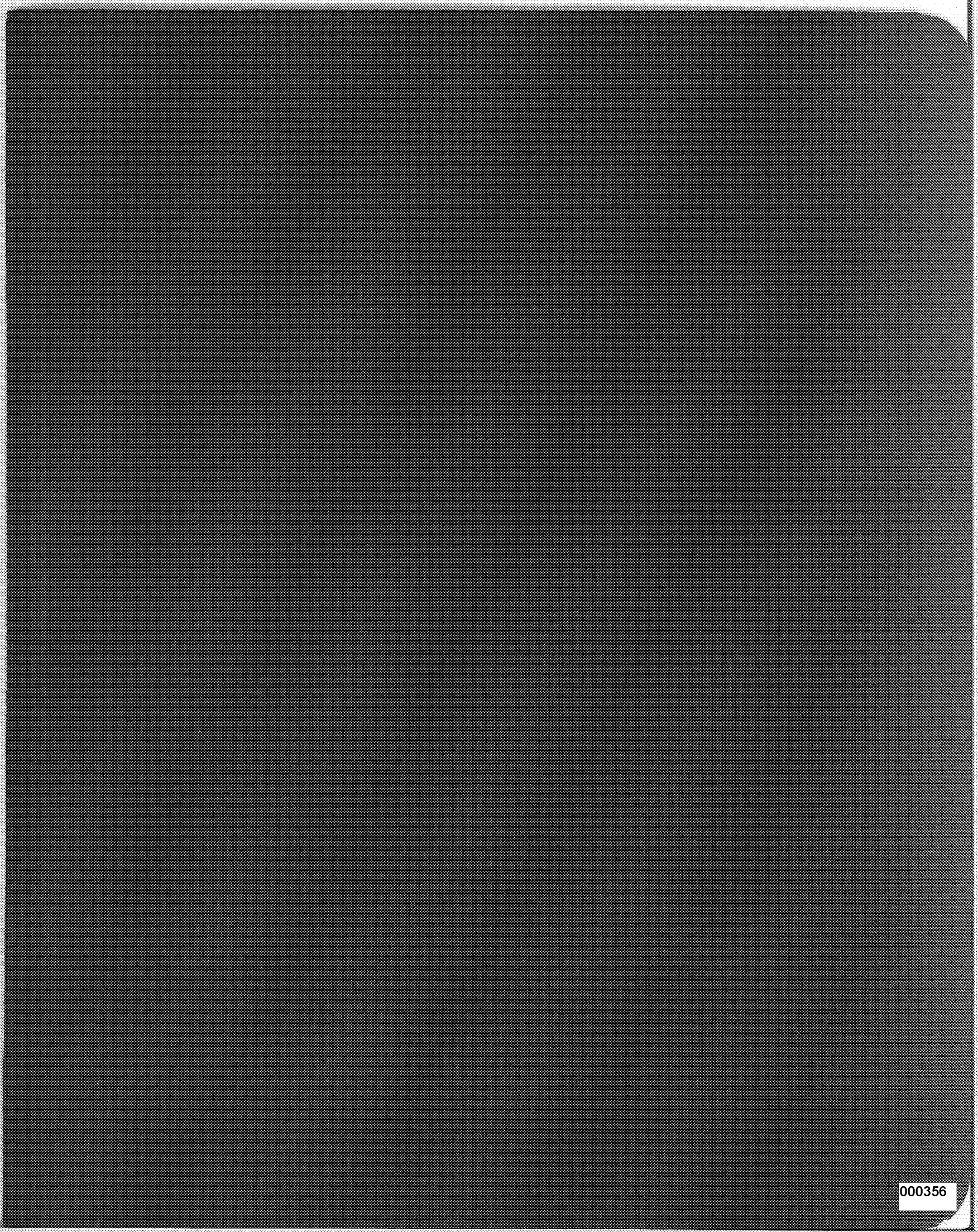
Date Mois Jour

Imprimer

Effacer

Envoyer par courriel

Merci de bien vouloir remplir ce formulaire. Pour nous l'envoyer, veuillez cliquer sur le bouton «Envoyer par courriel».



the Commissioner for the purpose of conducting that investigation.

2001, c. 41, s. 103.

2001, ch. 41, art. 103.

DIVISION 1

PROTECTION OF PERSONAL INFORMATION

Compliance with obligations

5. (1) Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1.

Meaning of "should"

(2) The word "should", when used in Schedule 1, indicates a recommendation and does not impose an obligation.

Appropriate purposes

(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

Effect of designation of individual

6. The designation of an individual under clause 4.1 of Schedule 1 does not relieve the organization of the obligation to comply with the obligations set out in that Schedule.

Collection without knowledge or consent

7. (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if

(*a*) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;

(*b*) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;

(*c*) the collection is solely for journalistic, artistic or literary purposes;

(*d*) the information is publicly available and is specified by the regulations; or

(*e*) the collection is made for the purpose of making a disclosure

SECTION 1

PROTECTION DES RENSEIGNEMENTS PERSONNELS

Obligation de se conformer aux obligations

5. (1) Sous réserve des articles 6 à 9, toute organisation doit se conformer aux obligations énoncées dans l'annexe 1.

Emploi du conditionnel

(2) L'emploi du conditionnel dans l'annexe 1 indique qu'il s'agit d'une recommandation et non d'une obligation.

Fins acceptables

(3) L'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Conséquence de la désignation d'une personne

6. La désignation d'une personne en application de l'article 4.1 de l'annexe 1 n'exempte pas l'organisation des obligations énoncées dans cette annexe.

Collecte à l'insu de l'intéressé et sans son consentement

7. (1) Pour l'application de l'article 4.3 de l'annexe 1 et malgré la note afférente, l'organisation ne peut recueillir de renseignement personnel à l'insu de l'intéressé et sans son consentement que dans les cas suivants :

a) la collecte du renseignement est manifestement dans l'intérêt de l'intéressé et le consentement ne peut être obtenu auprès de celui-ci en temps opportun;

b) il est raisonnable de s'attendre à ce que la collecte effectuée au su ou avec le consentement de l'intéressé puisse compromettre l'exactitude du renseignement ou l'accès à celui-ci, et la collecte est raisonnable à des fins liées à une enquête sur la violation d'un accord ou la contravention du droit fédéral ou provincial;

c) la collecte est faite uniquement à des fins journalistiques, artistiques ou littéraires;

d) il s'agit d'un renseignement réglementaire auquel le public a accès;

e) la collecte est faite en vue :

(i) under subparagraph (3)(*c*.1)(i) or (*d*)(ii), or

(ii) that is required by law.

Use without knowledge or consent

(2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if

(*a*) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention;

(*b*) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;

(*c*) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used;

(*c*.1) it is publicly available and is specified by the regulations; or

(*d*) it was collected under paragraph (1)(*a*), (*b*) or (*e*).

Disclosure without knowledge or consent

(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

(*a*) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization;

(*b*) for the purpose of collecting a debt owed by the individual to the organization;

(i) soit de la communication prévue aux sous-alinéas (3)*c*.1)(i) ou *d*)(ii),

(ii) soit d'une communication exigée par la loi.

Utilisation à l'insu de l'intéressé et sans son consentement

(2) Pour l'application de l'article 4.3 de l'annexe 1 et malgré la note afférente, l'organisation ne peut utiliser de renseignement personnel à l'insu de l'intéressé et sans son consentement que dans les cas suivants :

a) dans le cadre de ses activités, l'organisation découvre l'existence d'un renseignement dont elle a des motifs raisonnables de croire qu'il pourrait être utile à une enquête sur une contravention au droit fédéral, provincial ou étranger qui a été commise ou est en train ou sur le point de l'être, et l'utilisation est faite aux fins d'enquête;

b) l'utilisation est faite pour répondre à une situation d'urgence mettant en danger la vie, la santé ou la sécurité de tout individu;

c) l'utilisation est faite à des fins statistiques ou à des fins d'étude ou de recherche érudites, ces fins ne peuvent être réalisées sans que le renseignement soit utilisé, celui-ci est utilisé d'une manière qui en assure le caractère confidentiel, le consentement est pratiquement impossible à obtenir et l'organisation informe le commissaire de l'utilisation avant de la faire;

c.1) il s'agit d'un renseignement réglementaire auquel le public a accès;

d) le renseignement a été recueilli au titre des alinéas (1)*a*), *b*) ou *e*).

Communication à l'insu de l'intéressé et sans son consentement

(3) Pour l'application de l'article 4.3 de l'annexe 1 et malgré la note afférente, l'organisation ne peut communiquer de renseignement personnel à l'insu de l'intéressé et sans son consentement que dans les cas suivants :

a) la communication est faite à un avocat — dans la province de Québec, à un avocat ou à un notaire — qui représente l'organisation;

b) elle est faite en vue du recouvrement d'une créance que celle-ci a contre l'intéressé;

c) elle est exigée par assignation, mandat ou ordonnance d'un tribunal, d'une personne ou

(*c*) 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) 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;

(*c*.2) made to the government institution mentioned in section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* as required by that section;

*(*c*.2) made to the government institution mentioned in section 7 of the *Proceeds of Crime (Money Laundering) Act* as required by that section;

* [Note: Paragraph 7(3)(c.2), as enacted by paragraph 97(1)(*a*) of chapter 17 of the Statutes of Canada, 2000, will be repealed at a later date.]

(*d*) made on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization

(i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or

d'un organisme ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de documents;

c.1) elle est faite à une institution gouvernementale — ou à une subdivision d'une telle institution — qui a demandé à obtenir le renseignement en mentionnant la source de l'autorité légitime étayant son droit de l'obtenir et le fait, selon le cas :

(i) qu'elle soupçonne que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales,

(ii) que la communication est demandée aux fins du contrôle d'application du droit canadien, provincial ou étranger, de la tenue d'enquêtes liées à ce contrôle d'application ou de la collecte de renseignements en matière de sécurité en vue de ce contrôle d'application,

(iii) qu'elle est demandée pour l'application du droit canadien ou provincial;

c.2) elle est faite au titre de l'article 7 de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* à l'institution gouvernementale mentionnée à cet article;

c.2) elle est faite au titre de l'article 7 de la *Loi sur le recyclage des produits de la criminalité* à l'institution gouvernementale mentionnée à cet article;

* [Note : L'alinéa 7(3)c.2), édicté par l'alinéa 97(1)*a*) du chapitre 17 des Lois du Canada (2000), sera abrogé ultérieurement.]

d) elle est faite, à l'initiative de l'organisation, à un organisme d'enquête, une institution gouvernementale ou une subdivision d'une telle institution et l'organisation, selon le cas, a des motifs raisonnables de croire que le renseignement est afférent à la violation d'un accord ou à une contravention au droit fédéral, provincial ou étranger qui a été commise ou est en train ou sur le point de l'être ou soupçonne que le renseignement est afférent à la sécurité

Royal Canadian Mounted Police / Gendarmerie royale du Canada	ES&ML No: / No. des SE&LM: / Pages : 2	Security Classification : / Classification sécuritaire	**Protected A**

BRIEFING NOTE
TO THE MINISTER OF PUBLIC SAFETY

NOTE D'INFORMATION
AU MINISTRE DE LA SÉCURITÉ PUBLIQUE

ISSUE:

Whether to include in proposed legislation a requirement for telecommunication service providers in appropriate circumstances, to provide law enforcement agencies with customer information, e.g. names and addresses of customers.

BACKGROUND:

Currently in Canada there is no legal requirement for service providers to voluntarily provide customer information when requested to do so by law enforcement agencies. Increasingly, such information is not being provided. Service providers cite a number of concerns including potential civil liability.

The RCMP's National Child Exploitation Co-ordination Centre in Ottawa has reported that

It has been suggested that customer information should only be provided pursuant to a search warrant. However, a number of courts, including the Supreme Court of Canada in *R. v. Plant* [1993] 3 S.C.R. 281 have held that the type of information in question does not attract a reasonable expectation of privacy and therefore, there is no legal impediment to service providers releasing such information even when the request is not pursuant to a search warrant.

ANNEX

The attached Annex provides examples of situations where customer information has been requested by law enforcement agencies. In some cases the information requested was provided, and in some cases it was not. The Annex also includes an assessment of whether there was sufficient information available in each of the situations described to provide grounds for a warrant, had that been required.

RECOMMENDATION

It is strongly recommended that legislation be enacted to enable law enforcement agencies to access communications when authorized by law and that the legislation include provisions requiring telecommunication service providers to furnish customer name and address information in appropriate circumstances and subject to appropriate safeguards. It is further recommended that these safeguards not include a requirement for the obtaining of authorization by a court (i.e. a search warrant or a production order).

Prepared by : Rédigée par :	Recommended by : Recommandée par :		Approved by : Approuvée par :	Date
	Tim Killam Deputy Commissioner Policing Support Services	W.M. Sweeney Senior D/Commissioner	William J.S. Elliott Commissioner	09-05-11

In order to control the use of information, an approved caveat must be attached to all information that is shared with foreign law enforcement.

When sharing information with foreign law-enforcement agencies, investigators do so in writing and obtain approval from the Commander/Line Officer. In exigent circumstances, verbally, but documented then inform the Commander/Line Officer ASAP.

Caveat (App. 44-1-1)

The following caveat must be attached to all operational correspondence, messages and documents disseminated to foreign law-enforcement agencies.

> "This document and information contained therein is the property of the Royal Canadian Mounted Police (RCMP). It is loaned specifically to your agency in confidence and for law-enforcement purposes only. The document is not to be reclassified or further disseminated outside your agency and is not to be used in affidavits, or for other legal or judicial purpose without the written consent of the RCMP. This caveat is an integral part of this document and must accompany any extracted information. All reasonable steps shall be taken to ensure that the information is safeguarded against unauthorized disclosure. For any enquiries concerning the information or this caveat, please contact the originator."

Excerpts of RCMP policy
Sgt. Bernard Tremblay
2011-10-12

Disclosure of Personal Info by RCMP

SCAN

OM I.3.L

The disclosure of personal information must be made in accordance with the *Privacy Act*.

S. 8(1) forbids disclosure of personal information without the consent of the person to whom the information relates.

S. 8(2)(a) exception for: consistent use disclosure

- As law enforcement is considered one broad consistent use, the RCMP may collect personal information for one law enforcement purpose and release it for another law enforcement purpose.
- A member must not seek or collect personal information solely for the purpose of facilitating inquiries or investigations undertaken by another law enforcement or government agency. In such a case, a law enforcement or government agency should be advised to seek direct access to the desired information.
- Under the provisions of L.2.b.1., the RCMP may disclose personal information to the following agencies for legitimate investigative purposes in connection with their official duties and responsibilities relating to the enforcement or administration of the law:
    - Canadian law enforcement agencies and correctional services, and investigative, enforcement and support bodies of federal, provincial or territorial governments; and
    - foreign law enforcement agencies, correctional services, and investigative or enforcement bodies of government departments.
- Before releasing information or reports, a member must be satisfied that disclosure is in accordance with policy.

OM 44.1

Sharing of information with foreign law enforcement is done on a case-by-case basis, in compliance with applicable legislation considering the potential risk of mistreatment.

Before dissemination, the information must be assessed for: reliability, relevance (how the information might be used), accuracy, consistent use (to comply with privacy law).

From: Susan Alter
To: Tremblay, Bernard
Date: 10/5/2009 4:21 PM
Subject:

CC: Dodier, Amanda; Van Dyke, Helene

Hi Bernie,

Best regards,
Susan

Susan Alter, Senior Counsel /
Avocate-conseil
RCMP Legal Services /
Services juridiques GRC
Department of Justice /
Ministère de la Justice
Ottawa, Canada K1A 0R2

susan.alter@rcmp-grc.gc.ca
Telephone /Téléphone 613-990-9090
Facsimile /Télécopieur 613-990-2343
Government of Canada / Gouvernement du Canada

Questions et réponses – outil de déclaration en ligne des demandes de noms et d'adresses d'abonnés

(Compte rendu de la demande relative aux nom et adresse d'un abonné)

Q. 1. Qu'est-ce que l'outil de déclaration en ligne?

R. 1 L'outil de déclaration en ligne (Compte rendu de la demande relative aux nom et adresse d'un abonné) est un bref formulaire électronique qui est facile à remplir et qui permettra de documenter les réponses des fournisseurs de services de télécommunication (FST)* aux demandes concernant les noms et adresses d'abonnés. Ce formulaire permettra de recueillir des données importantes qui serviront à produire des preuves statistiques à l'appui des dispositions concernant les renseignements sur les abonnés qui font partie du projet de loi C-47 sur l'accès légal. Ces données feront état de réalités opérationnelles pertinentes, à savoir le nombre de demandes de communication des noms et adresses d'abonnés qui ont été acceptées, le nombre de demandes de ce genre qui ont été refusées et les répercussions de ces refus sur les activités policières qui ont donné lieu aux demandes (case 7 du formulaire), si elles sont connues. Par exemple, le compte rendu précisera si l'activité policière ayant donné lieu à la demande a cessé lorsque le FST a refusé de collaborer ou si elle a été retardée mais poursuivie.

Q. 2. Ne recueille-t-on pas déjà ce genre d'information?

R. 2. Le Centre national de coordination contre l'exploitation des enfants (CNCEE) de la GRC tient des données sur les demandes que les corps policiers transmettent aux FST dans les situations possibles d'exploitation d'enfants sur Internet, mais aucun renseignement n'est documenté relativement aux nombreux autres types d'enquêtes et de fonctions policières qui dépendent de l'obtention des noms et adresses d'abonnés. L'outil de déclaration en ligne permettra de recueillir des données sur les demandes présentées par la police dans toutes sortes d'enquêtes, notamment dans les domaines suivants :

- exploitation sexuelle d'enfants
- drogues et crime organisé
- enlèvements et personnes disparues
- fraude et criminalité financière
- autres

Q. 3 Nous avons déjà beaucoup à faire... pourquoi demandez-vous aux policiers de remplir un autre formulaire?

R. 3 Nous ne voulons pas alourdir votre fardeau administratif, mais la collecte de ces données revêt une importance capitale. Nous en avons besoin pour justifier les dispositions du projet de loi sur l'accès légal qui portent sur les renseignements concernant les abonnés. Sans données concrètes, il est entièrement possible que ces dispositions importantes mettent les intervenants politiques et le public mal à l'aise, réaction qui pourrait mener à leur suppression ou à la restriction considérable de leur portée. Notre travail à tous deviendrait

alors plus difficile dans les années à venir. La seule façon de recueillir ces données est de demander aux policiers du pays entier de prendre l'initiative de remplir le formulaire puis de nous l'envoyer. Le meilleur moyen de réfuter les critiques sans fondement est de présenter des faits, et le formulaire de déclaration en ligne nous fournira les faits nécessaires pour présenter des arguments vraiment convaincants à l'appui de la modification des dispositions législatives actuelles.

Q. 4 Combien de temps faut-il pour remplir le formulaire?
R. 4 Il ne faut qu'une ou deux minutes pour remplir le formulaire, qu'on peut envoyer par voie électronique à la Sous-direction des services d'enquêtes techniques de la GRC. Advenant l'adoption de la loi proposée sur l'accès légal, il faudra établir un mécanisme de déclaration quelconque de toute façon.

Q. 5 Dans la partie 1 du formulaire en ligne, il faut indiquer le type de demande : unique ou multiple. Qu'est-ce qu'une demande multiple?
R. 5 Il s'agit d'un lot de demandes relatives aux noms et adresses d'abonnés qui est envoyé par un intervenant appelé à soutenir les groupes d'enquête, par exemple le Centre national de coordination contre l'exploitation des enfants (CNCEE) ou un groupe des affaires spéciales I de la GRC. Dans ce genre de situation, on envoie une demande à un ou plusieurs fournisseurs de service afin d'obtenir les noms et adresses de plusieurs abonnés en même temps. Étant donné que la plupart des enquêteurs de première ligne ne présentent que des demandes uniques, ils rempliront un formulaire de compte rendu pour chaque demande relative aux nom et adresse d'un abonné.

Q. 6 Ce projet commence à compter de maintenant. Que dois-je faire si j'ai des renseignements au sujet de demandes présentées antérieurement à des FST?
R. 6 Si vous avez des renseignements au sujet de demandes que vous avez faites au cours de la dernière année civile, veuillez remplir un formulaire à leur sujet et nous l'envoyer.

Q. 7 Que dois-je faire si je travaille dans une région du pays où je sais que les FST ne fournissent jamais les noms et adresses de leurs abonnés volontairement? Autrement dit, s'ils exigent toujours un mandat?
R. 7 Nous vous demandons de remplir le formulaire en ligne et de nous l'envoyer quand même. Ces comptes rendus nous permettront de savoir combien de fois la police est obligée de demander une ordonnance au tribunal parce qu'elle n'a pas le choix de procéder autrement.

Q. 8 Qui utilisera cet outil en ligne?
R. 8 Il faut faire remplir le formulaire par tous les agents ou les employés de corps policiers qui présentent des demandes de ce genre à des FST, et ce, dans l'ensemble du pays. Cette participation sera extrêmement importante plus tard, quand viendra le temps de faire comprendre aux législateurs et au public

pourquoi l'adoption de la loi proposée nous permettra de faire notre travail plus efficacement.

Q. 9 Pendant combien de temps devrons-nous remplir ce formulaire?
R. 9 Jusqu'à ce que la loi soit adoptée. Lorsque les intervenants politiques, les médias et le public sauront que nous recueillons ces données, ils demanderont des mises à jour régulières. Une fois la loi adoptée, il faudra mettre au point de nouveaux formulaires, et de nouveaux rapports seront produits relativement aux demandes de renseignements sur les abonnés.

Q. 10 Qui se chargera de compiler les résultats et à quoi serviront les statistiques?
R. 10 - Des membres de la Sous-direction des services d'enquêtes techniques de la Direction des opérations techniques de la GRC, à Ottawa, recevront les formulaires et en compileront les données. Celles-ci serviront à justifier le maintien des dispositions sur les renseignements concernant les abonnés dans le projet de loi C-47 ou à encourager davantage de FST à fournir de tels renseignements lorsqu'on en fait la demande.

Selon le Centre national de coordination contre l'exploitation des enfants (CNCEE) de la GRC, qui tient des statistiques sur les demandes relatives aux noms et adresses d'abonnés, le taux de refus de ces demandes s'élevait à 31 % en 2007 et à 24 % en 2008. On croit que ce taux serait beaucoup plus élevé s'il tenait compte de toutes les demandes de noms et d'adresses d'abonnés; c'est pourquoi on demande la collecte de données sur les demandes de ce genre qui sont présentées dans divers contextes d'enquête.

Q. 11 Pourquoi nous demande-t-on de remplir ce formulaire maintenant?
R. 11 Nous avons beaucoup de preuves empiriques, mais ce n'est pas suffisant. Comme nous l'avons déjà mentionné, il nous faut des données concrètes pour justifier le bien-fondé du projet de loi C-47 à mesure qu'il avance dans le processus législatif, et le seul moyen d'en obtenir est de compter sur votre collaboration.

Q. 12 Au fait, pourquoi les FST devraient-ils être tenus de fournir les noms et adresses de leurs abonnés sans ordonnance du tribunal?
R. 12 Comme vous le savez, il n'est pas toujours possible d'obtenir une ordonnance judiciaire au début d'une enquête criminelle; parfois, à ce stade, la police n'a pas encore recueilli assez d'information pour avoir des motifs de demander une ordonnance au tribunal. D'autre part, il est impossible d'obtenir une telle ordonnance dans l'exercice de fonctions policières générales, car aucune infraction criminelle ne fait alors l'objet d'une enquête.

Qu'il s'agisse d'une enquête ou de fonctions policières générales, la police constate généralement, lorsqu'elle présente sa demande au tribunal, que la loi n'exige pas la présentation d'un mandat ou d'une autre ordonnance judiciaire

pour obtenir des renseignements de base sur un abonné, tels que son nom et son adresse. Le formulaire utilisé par les groupes de lutte contre l'exploitation d'enfants dans Internet pour demander aux fournisseurs d'accès Internet (FAI) de communiquer volontairement les noms et adresses d'abonnés aux fins d'enquêtes sur l'exploitation sexuelle d'enfants a d'ailleurs résisté à de nombreux examens en vertu de la Charte en 2008 et en 2009.

Q. 13 Est-ce que ça vaut la peine de faire tout ça maintenant que le Parlement a été prorogé?

A. 13 Oui. Cependant, bien que nous espérons que le projet de loi sera réintroduit lorsque le Parlement reprendra, nous ne savons pas si ce sera le cas, ni si les dispositions d'un nouveau projet de loi seraient identiques à celles de C-47. Pendant cette période d'incertitude, la GRC aimerait profiter de cette pause dans le processus législatif pour obtenir de l'information supplémentaire et de meilleure qualité pour démontrer qu'il existe un besoin pour cette loi.

Le terme « fournisseur de services de télécommunication » (FST) englobe les compagnies de téléphone et les fournisseurs d'accès Internet (FAI).

Questions and Answers - CNA on-line Reporting Tool

(Record of Customer Name and Address (CNA) Request)

Q. 1. What is the on-line reporting tool?

A. 1 The on-line reporting tool (Record of Customer Name and Address (CNA) Request) is a short, user friendly electronic form which, when completed by police, will document Telecommunications Service Providers' (TSPs)* responses to requests for CNA information. This form will collect important data that will be used to produce statistical evidence supporting the case for the subscriber information provisions in the lawful access legislation (Bill C-47). The data will reveal important operational facts such as how often police requests for CNA information are granted or refused and the impact of the refusals. It will record the impact, if known, on the police work behind the query – (Box 7 on form) The report will indicate, for example, if the police work related to the CNA query stopped with the TSP's refusal to assist or it was delayed but carried on)

Q. 2. Isn't this type of information collected already?

A. 2. The RCMP's National Child Exploitation Coordination Centre (NCECC) maintains data on law enforcement requests (LERs) to TSPs in possible instances of on-line child sexual abuse, but there is no data available for the many other types of investigations and other policing duties that rely on CNA information. The on-line reporting tool will provide data as it relates to law enforcement requests from all manner of investigations including:

- Child sexual exploitation
- Drugs and organized crime
- Abduction/missing persons
- Fraud/financial crime
- Other

Q. 3 We're busy already...why are you asking police to fill-in another form?

A. 3 We're not trying to burden you with more paperwork, but gathering this kind of data is extremely important. We need it to justify the subscriber information provisions in the lawful access bill. Without hard data, there is a real risk that politicians and the public will not be comfortable with these important provisions and, as a result, they could be lost or severely watered down. And that will make all our jobs more difficult in the future. The only way to collect this data is for police across the country to step up and complete the form and send it back to us. The best way to counter unfounded criticism is with facts – the on-line reporting form will provide the facts we need to make a really compelling case for the necessary changes to the law.

Q. 4 How long will it take to fill out the form?

A. 4 The form takes no more than a minute or two to complete and can be sent electronically to the RCMP's Technical Investigations Services Branch. When

and if lawful access legislation is passed, some manner of reporting mechanism will be required in any case.

Q. 5 In section one of the on-line form you're asking "what type of request this is?...single or multiple." What do you mean by a "multiple" request?
A. 5 Multiple requests are "batch" requests for CNA information that are made by centres that play an investigative support role for investigational units, for example the National Child Exploitation Coordination Centre and Special "I" Units of the RCMP. They are a query sent to one or more service providers for the CNA of a number of customers, all at the same time. Most front-line investigators normally would only be making single requests and so they would submit a CNA request report for each individual request they make.

Q. 6 This project is just starting now. What if I have information from past requests I've made to TSPs?
A. 6 If you have information from requests you've made anytime in the past calendar year, please complete a form and send it back.

Q. 7 What if I'm working in a part of the country where I know TSPs will never provide CNA information voluntarily? That is, they always demand a warrant?
A. 7 We ask that you complete a CNA report anyway and send it back via the on-line reporting tool (form). These reports will give us data on how many times police have to apply to a court for an order because they have no other option.

Q. 8 Who will be using this on-line tool?
A. 8 We need every officer or police service employee across Canada who deals with the TSPs on these issues to complete the form. It's going to be extremely important down the road in getting legislators and the public to understand why we need the new legislation to do our jobs more effectively.

Q. 9 How long are we expected to continue to complete these forms?
A. 9 Until such time as the law is passed. Once politicians, the media and the public know we are collecting it they will ask for regular updates on the data. Once the law is passed new forms will be required and new reports will be generated related to subscriber information requests.

Q. 10 Who is compiling the results and what will be done with the statistics?
A. 10 - RCMP members of the Technical Investigations Services Branch of Technical Operations in Ottawa will receive and compile the results from the forms submitted. The data will be used to support the case for the subscriber information provisions in Bill C-47 or to encourage more ISPs to provide CNA information when requested.

The RCMP's National Child Exploitation Coordination does keep CNA statistics and reports that non-cooperation rates for CNA requests were 31 per cent and 24 per cent respectively for 2007 and 2008. It's believed non-cooperation rates from ISPs would be significantly higher if the results of all CNA requests were taken into account; thus the reason for collecting CNA request from a broad range of investigations.

Q. 11 Why are we being asked to do this now?
A. 11 We have lots of anecdotal evidence, but that's not enough. As mentioned earlier, we have to have hard data to support Bill C-47 as it goes through the legislative process and the only way to get that data is with your cooperation and assistance.

Q. 12 Why should TSPs be required to provide CNA information without a court order anyway?
A. 12 As you know, obtaining court orders in the early stages of a criminal investigation may not always be possible, as the investigation may not have developed to the point where police have gathered sufficient information to meet the grounds necessary to apply to a court for an order. In addition, obtaining court orders for general policing duties is not possible because no criminal offence is under investigation; hence seeking an order of the court is not an option.

For either purpose, investigative or general policing duties, it is the experience of police in most courts that the law does not require a warrant or other court order for basic customer identifying information such as CNA. The Law Enforcement Request form, which Internet Child Exploitation (ICE) units use to ask Internet Service Providers (ISPs) to voluntarily disclose CNA for child sexual exploitation investigations, has held up to Charter scrutiny in numerous cases in 2008 and 2009.

Q. 13 Is there any point to doing this now that Parliament has been prorogued?
A. 13 Yes. However, while we hope the Bill will be reintroduced when Parliament resumes, there are no guarantees that it will be or, if it is, that the new bill will be the same as Bill C-47. During this period of uncertainty, however, RCMP would like to take advantage of the break to gather more and better information to demonstrate the need for such legislation.

Telecommunications Service Providers (TSPs) includes both Telephone Companies and Internet Service Providers (ISPs)

January 2010

Article documentaire sur les noms et adresses d'abonnés

Depuis 1999, la GRC collabore avec Sécurité publique Canada, le Service canadien du renseignement de sécurité (SCRS), le ministère de la Justice et Industrie Canada pour combler les lacunes de la législation actuelle en ce qui concerne la capacité des organismes d'application de la loi à intercepter légalement les communications et à obtenir légalement des renseignements sur les abonnés. En l'absence de lois canadiennes sur l'accès légal, il est souvent impossible d'obtenir, du moins immédiatement, l'autorisation judiciaire requise en vue de l'interception de communications. De plus, faute de dispositions législatives l'autorisant explicitement à obtenir sur demande des renseignements concernant les abonnés, la police se voit souvent obligée d'obtenir une ordonnance du tribunal pour avoir accès à ces renseignements, par exemple aux nom et adresse d'un abonné, si le fournisseur de services de télécommunication (FST)* refuse de collaborer. Le projet de loi C-47, tel qu'il est présentement, conférerait aux autorités policières les pouvoirs nécessaires pour obtenir des renseignements sur les abonnés des compagnies de téléphone et des fournisseurs d'accès Internet (FAI)*.

Le projet de loi a franchi l'étape de la deuxième lecture avant la prorogation récente du Parlement. Nous espérons qu'il sera réintroduit lorsque le Parlement reprendra mais nous ne savons pas si ce sera le cas, ni si les dispositions d'un nouveau projet de loi seraient identiques à celles de C-47. Pendant cette période d'incertitude, la GRC aimerait profiter de cette pause dans le processus législatif pour obtenir de l'information supplémentaire et de meilleure qualité pour démontrer qu'il existe un besoin pour cette loi.

Documentation d'exemples à l'aide d'un formulaire de déclaration en ligne

En raison des questions de respect de la vie privée que soulèvent les dispositions proposées au sujet des renseignements sur les abonnés, il importe de recueillir des données concrètes pour pouvoir citer des exemples de situations où un FST a refusé de fournir le nom et l'adresse d'un abonné. C'est pourquoi la GRC demande à la collectivité d'application de la loi, plus précisément aux agents qui demandent des renseignements sur les abonnés aux FST dans le cadre de leurs enquêtes et de leurs fonctions policières générales, de remplir un formulaire de déclaration en ligne. Ce formulaire ne prend qu'une ou deux minutes à remplir et nous aidera à recueillir les données nécessaires pour fournir des preuves statistiques à l'appui de l'adoption des dispositions du projet de loi C-47 qui concernent l'accès légal aux renseignements sur les abonnés.

La GRC compte aussi faire appel à l'Association canadienne des chefs de police (ACCP) pour encourager la collectivité policière à rassembler des exemples de situations d'enquête ou autres où des agents ont demandé les nom et adresse d'un abonné à une compagnie de téléphone ou à un FAI mais n'ont pas réussi à

obtenir sa collaboration. Nous désirons également obtenir des exemples de réussites, c'est-à-dire de situations où un FST a accepté volontairement de communiquer des renseignements à la police. Ces exemples aideront le Parlement et le public à comprendre comment la police cherche à obtenir des renseignements de ce genre auprès des compagnies en cause, le but dans lequel elle fait ces démarches et les raisons pour lesquelles il n'est pas toujours pratique ou possible d'obtenir un mandat à cette fin. Ils contribueront ainsi de façon très importante à améliorer la compréhension du projet de loi C-47.

Nous demanderons par ailleurs l'aide de l'ACCP pour intégrer ces exemples à des déclarations publiques une fois qu'ils auront été recueillis par la GRC.

La vérité sur le projet de loi C-47

Quelques précisions

- La loi proposée n'établit aucun nouveau pouvoir en vue de l'interception de communications. La police devra encore obtenir une ordonnance du tribunal à cette fin.

- Le projet de loi C-47 mettra à jour la législation actuelle en fonction des réalités du 21e siècle, de l'évolution de la technologie et des menaces accrues qui en découlent pour la sécurité publique.

- La législation actuelle n'oblige pas les compagnies de télécommunication à doter leurs systèmes de mécanismes d'interception intégrés. Le projet de loi C-47 amènerait graduellement ces compagnies à incorporer de telles capacités à leurs systèmes.

- Le projet de loi C-47 prévoit certaines mesures préconisées par les commissaires à la protection de la vie privée, par exemple l'obligation de documenter l'origine des demandes d'information, de faire des vérifications et de surveiller le traitement de l'information.

- Les nom et adresse d'un abonné n'étant que des coordonnées, ils ne sont pas considérés comme des renseignements biographiques de base sur la personne visée. En effet, l'information de ce genre n'est pas confidentielle; facile à obtenir, elle peut même être accessible au public. L'historique des conversations en ligne ou la liste des sites Web visités ne font certainement pas partie des renseignements que la police pourra obtenir sur demande au sujet d'un abonné.

- La communication des nom et adresse d'un abonné porte encore moins atteinte à la vie privée de ce dernier que la vérification d'un numéro de

plaque d'immatriculation. Comparativement aux activités qui nécessitent l'obtention d'une ordonnance du tribunal, comme l'écoute électronique ou la perquisition d'une résidence, l'obtention de ces renseignements n'a rien d'envahissant du tout.

- La police a besoin de pouvoir obtenir les noms et adresses d'abonnés dans l'exercice de ses fonctions quotidiennes. L'outil de déclaration en ligne nous en dira beaucoup plus long sur le genre de situations où la police demande les nom et adresse d'un abonné sans d'abord obtenir un mandat. Voici quelques exemples de situations où la police peut devoir faire une telle demande :

  - exploitation sexuelle d'enfants
  - drogues et crime organisé
  - enlèvements et personnes disparues
  - fraude et criminalité financière
  - autres

- Certains FAI refusent d'accéder aux demandes présentées par des policiers en vue d'obtenir les nom et adresse d'un abonné sans mandat, même si aucun mandat n'est requis pour la communication de ce genre d'information.

- Il persiste une réticence à collaborer volontairement avec la police lorsqu'elle demande les nom et adresse d'un abonné. Dans certaines régions, notamment dans l'Atlantique, tous les FAI exigent la présentation d'un mandat avant d'accéder à ces demandes.

- Certains FAI, mais pas tous, reconnaissent leur devoir social de collaborer avec la police dans le cadre de ses activités de dépistage et de prévention du crime ainsi que lors des étapes préliminaires d'une enquête.

- Le refus des FST de collaborer avec la police peut entraîner une augmentation du nombre de crimes commis et de personnes qui en sont victimes.

* Le terme « fournisseur de services de télécommunication (FST) » englobe les compagnies de téléphone et les fournisseurs d'accès Internet (FAI).

From: John Roskam
To: Bernard Tremblay; William Milley
Date: 9/24/2009 12:58 PM
Subject: Re: ISPs in Toronto

Our girls are very efficient.
Not sure how accurate this is but we Googled it and the response was 59 ISP's for the GTA. We do not have contacts for all of them.

Regards
John

>>> William Milley 2009-09-24 12:45 >>>
I don't but give John Roskam in Newmarket Special "I" a call, (905) 953-7611 (416) 346-3239 cell.
Regards, BIII

>>> Bernard Tremblay 2009-09-24 1:14 PM >>>
Hi Bill,

Would you know how many (roughly) ISPs there are in the Greater Toronto Area? If you don't know, do you know who I could ask?

Bernie

Bill C-47 - CNA Reporting Tool - NIOC Video Conference 2009-10-28

As discussed during the video conference of 2009-10-28, chaired by D/Commr. Killam, attached are relevant documents outlining background information, along with expected results of this initiative. As you know, Deputies Killam and Souccar fully endorse the extra efforts required by front line Units in order to assist Tech Ops in providing meaningful statistics to our Minister, in support of Bill C-47. To this end, the RCMP has created form 6306, Record of Customer Name and Address (CNA) Request, currently available on-line via the Web Forms Catalogue.

Law Enforcement Agencies (LEA) in Canada, along with support from the CACP, have long lobbied for enhancements to electronic surveillance provisions, or more precisely, the lack of adequate provisions. The ***Technical Assistance for Law Enforcement in the 21st Century Act*** (Bill C-47) will provide us with a number of appropriate tools and methods which will enable the Law Enforcement community to maintain an operational advantage when faced with the fast paced advances in technology.

C-47 has undergone second reading in the House of Commons and has been referred to the Standing Committee on Public Safety and National Security (SECU). It is expected SECU will begin scheduling and hearing from witnesses in the near future. Based on the debates during second reading, privacy issues regarding the warrant-less authority to obtain customer name and address (CNA) information are expected to be at the forefront. The CNA Reporting Tool has been designed to gather statistics and capture a snapshot on the level of cooperation between LEA and the Telecoms Service Providers (TSP).

To complement these statistics, we are also gathering examples of instances where CNA information was sought, the outcome, and how this outcome impacted the investigation. Currently, the NCECC has been the only Unit compiling statistics on CNA requests, but it is hoped that examples related to other types of investigations will provide a better cross section view of how informal CNA requests can assist or impede investigations.

In the near future, you will also be provided with a few examples of investigations where CNA requests were submitted, along with the resulting effects. In addition, more examples of CNA refusal or success stories are required. The Minister and other Senior resources rely on these to show real life situations where TSP cooperation or non-cooperation has had a real impact on investigations (examples from Nation al Security and Federal Investigations would be appreciated). We are also accepting examples of CNA requests that occurred in the last calendar year. Without these examples, it will be difficult to support our claim that there is a need for a legislated obligation to provide CNA information to law enforcement upon request and without a court order.

With the support of Deputies Killam and Souccar, I am counting on your collaboration by providing us with the requested statistics and, where appropriate, examples outlining the results of these informal requests and how the investigation was impacted (positive or negative). Your assistance is appreciated and will undoubtably serve our Minister well as this legislation is processed through Parliament.

Privacy Comm'r.

Q.

From: Mike Gaudreau
To: Bernstein, Elisa
CC: rainville, Donna
Date: 7/26/2009 11:44 AM
Subject: Fwd: C-46 and C-47

Elisa,

Please prepare the response to the questions noted so I may review and submit to C/Supt. Giguere.

Although there was no DD attached, I would appreciate it being done by COB this Thursday, July 30th.

Merci

Mike

>>> Pierre Giguere 7/24/2009 2:57 PM >>>
Mike,
pourrais-tu produire les réponses recherchées .

Merci

Pierre

>>> 7/24/2009 2:49 PM >>>
Good afternoon Bruce,

First I want to tell you how helpful we found our meeting with you and your staff last July 7. Thank you very much. Since we have met with you, we have also met with representatives from the industry and we will meet with representatives from civil society and police associations in the coming weeks.

As we are pursuing our analysis of the Bills, the following questions arise that I share with you in the hope you can address them and help us progress:

Bill C-47:

* Would the adoption of the legislation, and in particular section 16, markedly increase the requests by police for subscriber information? If so, on the basis of your current experience, do you have any estimation of potential increase in requests?
* Also on the basis of your experience, what type of offences are usually at the root of a request for subscriber information?
* How will police services make known the identity of "designated persons" under section 16? We assume this will be dealt with in regulations - has it been discussed already?
* Exactly why has the option of restricting section C-47 to only serious offences been considered "unworkable"?

C-46:

* Technically, what does the term "activate" refer to in relation to tracking devices? In other words what does it add to the current Criminal Code provisions?

We also need clarification on the oversight regime but will address our questions to Public Safety.

I would be very grateful if you or one of your staff could get back to me - by email is best.

Thank you very much.

Royal Canadian Mounted Police / Gendarmerie royale du Canada	File No. / N° de dossier	Security Classification/Designation / Classification/désignation sécuritaire	Total Pages / Pages totales
		Secret	2

BRIEFING NOTE TO THE DEPUTY COMMISSIONER — **NOTE D'INFORMATION AU SOUS-COMMISSAIRE**

REINTRODUCTION OF LAWFUL ACCESS LEGISLATION

PURPOSE:

- To brief the Commanding Officer "E" Division on the pending reintroduction of Lawful Access Legislation.

BACKGROUND:

- The *Modernizing Criminal Investigation Powers Act* groups together three former bills (C-50, C-51 and C-52) which were introduced in 2010 but subsequently died on the Order Paper when Parliament dissolved on March 26, 2011.
- This bill contains:
  - Amendments to the *Criminal Code* [formerly C-50]
    - Police may group together applications for court orders related to the same wiretap investigation, ensuring consistency regarding process, duration and sealing.
    - Safeguards consisting of annual reporting and notification of persons intercepted are added to s. 184.4 CC interceptions (exceptional circumstances).
  - Amendments to the *Criminal Code*, the *Competition Act* and the *Mutual Legal Assistance in Criminal Matters Act* [formerly C-51]
    - Modernizes the *Criminal Code* provisions to allow police to obtain transmission data that is received or sent via the telephone or Internet.
    - Creates Preservation demands and orders to compel telecommunications service providers to preserve, for a specified period of time, computer data related to specific communications or subscribers.
    - Updates tracking warrant provisions to take account of new technological developments.
    - Allows Canada to ratify the Council of Europe *Convention on Cybercrime* (ETS-185).

Submitted by – Rédigé par:	Date	Recommended by – Recommandé par:	Date
C/Supt. Stan Burke D.G. Technical Investigation Services Director (or DG)		Antoine Babinsky A/Commr. Technical Operations Service Line Leader	11-12-13
Approved by – Approuvé par Line Carbonneau, D/Commr. Policing Support Services	Date	Reviewed by – Examiné par	Date

- Widens the scope of assistance that Canada can provide to its international partners.

- Creation of the *Investigating and Preventing Criminal Electronic Communications Act* (IPCECA) [formerly C-52]
  - Telecommunications service providers (TSPs) must build and maintain intercept capable networks.
  - TSPs must provide Police, CSIS and Competition Bureau with basic subscriber information upon request (no need for court order).

CURRENT STATUS:

- The *Modernizing Criminal Investigation Powers Act* is expected to be reintroduced in Parliament in early 2012.