

Lawful Access and Small Service Providers

In general, ISPs support lawful access and the need for LEAs and national security agencies to undertake lawful interception.

General concerns with proposed changes:

- Is there really a need for expanded intercept capabilities?
- What technical standards will be adopted and how/by whom will those standards be implemented?
- Cost of hardware, cost of training, cost of administration, cost of...: no details on how expanded capabilities will be paid for.
- Implementation timelines and exemptions.
- Consumer privacy, consumer perception.

eagle.ca



Lawful Access Requests... are they really increasing?

- The Solicitor General's Annual Report on the Use of Electronic Surveillance shows a general decrease in applications, arrests and notifications from 1996 to 2005

1996	1997	1998	1999	2000	2001	2002	2003	2004	2005
TOTAL APPLICATIONS MADE									
281	193	162	154	150	152	180	110	141	106
NUMBER OF INTERCEPTIONS									
1157	1624	1065	1149	1718	1203	2131	1473	1237	696
TOTAL ARRESTS MADE									
790	625	273	439	313	380	600	373	320	81
NOTIFICATION OF SUBJECTS OF INTERCEPTIONS									
1991	1448	995	949	390	1108	856	1977	1082	596

eagle.ca



Costs

- Small ISPs often purchase equipment for expansion on the secondary market
 - Hardware that is 5+ years old is deployed on a regular basis
 - Margins are small (and shrinking) on many services
- Cost of compliance *will* force some ISPs out of business
- If the goal is to combat crime then costs should be recovered through "proceeds of crime" funds not through ISP margins or price increases borne by consumers

eagle.ca



Standards

- Global standards for interception not yet established for hardware manufacturers to build to...
 - Canada cannot have a *Maple Leaf Solution*. Major manufacturers build to global standards.
 - There has been little discussion of what constitutes a solution (OEM, third-party, retrofits)
 - What guarantee do TSPs have that hardware they deploy to meet compliance requirements will keep us in compliance in the future... or will we have to re-comply when another new technology is introduced?

eagle.ca



Exemptions and Timelines

- In the discussions held with Government over the last few years a number of exemptions were discussed, including TSPs with less than 100,000 subscribers
 - Most small ISPs have never been asked to assist with an intercept
- Discussions moved from compliance being required for new additions in networks over a period of years to overall compliance within months.
 - The need to retrofit or replace hardware within a short timeframe will create financial hardship for many small ISPs

eagle.ca

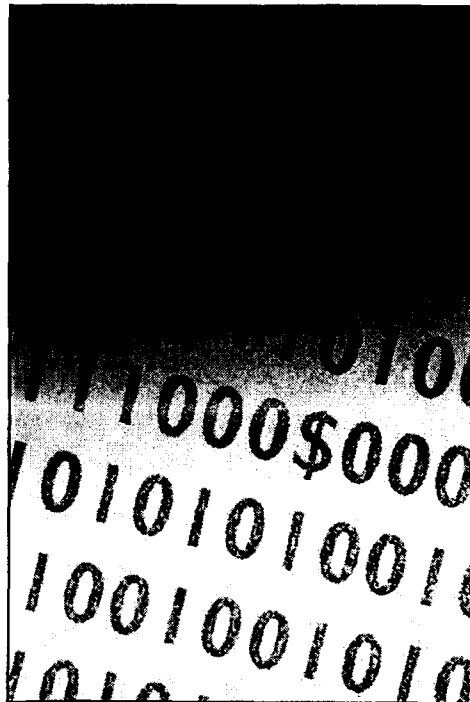


Consumer privacy, consumer perception

- ISPs have a long standing tradition of zealously protecting our customers' privacy
- Many have had little or no experience with lawful intercepts in the past
 - They have neither the legal or operational resources to be able to effectively comply with requests in a timely manner
- Some consumers would see their ISP as an agent of law enforcement



eagle.ca



CAIP
Canadian Association
of Internet Providers
a division of
CAI Alliance



ACFI
Association canadienne
des fournisseurs Internet
une division de
CAI Alliance

Tom Copeland, Chair
388 Albert Street
Ottawa, ON, CA
K1R 5B2

Phone: 01-613-232-2247

Direct: 01-905-373-9313

www.caip.ca

tom.copeland@eagle.ca

eagle.ca

Mr. Brian A. Tabor, Q.C.
President
Canadian Bar Association
865 Carling Avenue, Suite 500
Ottawa, ON K1S 5S8

Dear Mr. Tabor:

Thank you for your correspondence of July 5, 2006, on behalf of the Canadian Bar Association (CBA), raising privacy concerns related to Internet Service Providers (ISPs) amending their service agreements with customers and, more specifically, announcing that they will “monitor or investigate” how customers use their services and “disclose any information necessary to satisfy” governmental legislation.

At the outset, I would like to emphasize that intercepting private communications is an offence in Canada unless it is done in conformity with the *Criminal Code* and other laws of Canada. I do not, however, wish to specifically comment on the revision of service agreements by ISPs and whether or not they are related to government legislation since I am not in a position to speculate on why certain corporations decided to make changes to their ISP subscriber agreements. These questions may be more adequately addressed to the ISPs themselves. In addition, I will leave comments regarding former Bill C-74, the *Modernization of Investigative Techniques Act* (MITA), a bill that died on the order paper last fall, to my colleagues the Honourable Stockwell Day, Minister of Public Safety, and the Honourable Maxime Bernier, Minister of Industry, since the issues that were covered in this bill fall within their purview.

As the CBA is aware, in 2002 and 2005, the Government of Canada held extensive public consultations on the lawful access initiative. The Government continues to consider measures to address the issues raised; while these measures may at some point include legislative proposals, the timeframe has yet to be determined. As Minister of Justice and Attorney General of Canada, I cannot agree more with the importance of the Government adopting measures that conform with legal protections and guarantees that safeguard Canadians’ rights and freedoms. It is my responsibility to ensure that any updates to legislation to keep pace with new and emerging forms of technology respect the principles of privacy and human rights which are entrenched in laws such as the *Canadian Charter of Rights and Freedoms*, the *Privacy Act*, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and preserve the delicate balance between these rights and the safety of our citizens.

With respect to the issue of solicitor client privilege, my departmental officials have been assessing whether amendments to the *Criminal Code* are necessary to respond to the Supreme Court of Canada's decision in *Lavallee*. The Department released a comprehensive consultation paper on this issue to key justice system stakeholders, including the Canadian Bar Association, and had asked for responses by December 2005. A number of submissions have been received from a range of stakeholders, although the Department has not yet received a response from the CBA and would certainly welcome your submissions on the issues that are important for the legal profession.

My departmental officials and I always appreciate opportunities to discuss issues of mutual concern with the Canadian Bar Association, as I indicated at your recent annual meeting in St. John's in August. In addition, my officials will be happy to discuss the concerns of your organization at the upcoming annual section meetings this fall. Finally, please feel free to contact Mr. Bill Pentney, Senior Assistant Deputy Minister, Department of Justice Canada, at (613) 957-4725, should you require any additional information in relation to the *Criminal Code* component of the lawful access initiative.

Thank you again for writing on this important issue.

Yours sincerely,

Vic Toews

c.c.: The Honourable Maxime Bernier, P.C., M.P.
 The Honourable Stockwell Day, P.C., M.P.

**PROPOSED STAKEHOLDERS TO BE INVITED TO TECHNICAL BRIEF
ON DAY OF INTRODUCTION**

Total = 46 + GoC

Telecommunications Service Providers (16)

Information Technology Association of Canada (ITAC)	Bill Munson, ED Policy and Planning
Canadian Wireless Telecommunications Association (CWTA)	J. David Farnes, VP Industry & Regulatory Affairs
Canadian Cable Telecommunications Association (CCTA)	Jay Kerr-Wilson, VP Legal Affairs
Canadian Advanced Technology Alliance (CATA)	Kirsten Embree, Partner, Frasier Milner Casgrain
Bell Canada	David Elder, VP Regulatory Law
Bell Mobility	Kelly Hisaki
Telus	Ed Prior
Telemobile	Parke Davis, Senior Regulatory Advisor
Rogers	Jennifer Warren, VP and Assistant General Counsel
Rogers Wireless	Joel Thorpe, Director Inter-carrier Relations
Cogeco	Mike Coltart, Manager Security and Carrier Services
MTS Allstream	Chris Schmitt, Director Regulatory Affairs
Telesat	Robert Power, Director, Regulatory and Government Initiatives
Shaw	Cynthia Rathwell
Vidéotron	Serge Sasseville
Primus	Terrie-Lynn Devonish, General Counsel

Vendors/Solution Providers (7)

Nortel	Pete Streng, Product Manager
SS8	Karen Miller, Senior Account Executive
TopLayer	Kyriacos (Ken) Georgiades, Sen.Dir. IP Intercept Product Line
Juniper	Douglas Linder, Manager, Systems Engineering
Cisco	Keith Tyndall, Service Provider Operations
Ericsson	Donald Hartung, Manager Combined Products
Verint	Todd McDermitt

Privacy Stakeholders/Civil Society Advocates/Others (9)

Office of the Privacy Commissioner of Canada	Stephanie Perrin
Canadian Bar Association	Joshua Hawkes
Canadian Internet Policy and Public Interest Clinic (CIPPIC)	Phillipa Lawson
Civil Liberties Association, National Capital Chapter	Leo Lehtiniemi
Freedom of Information and Privacy Association (FIPA)	Darrel Evans, Executive Director

**Option Consommateurs
University of Ottawa**

Jannick Desforges, avocate
Michael Geist, Law Professor and Research
Chair for Internet and E-Commerce Law or

**Public Interest Advocacy Centre (PIAC)
Wesley Wark**

John Lawford

Police and Provinces (14)

CACP Vince Westwick (6 total)

Alberta SG Brian Skeet

Ontario AG Catherine Cooper

Quebec AG Pierre LaPointe

RCMP (2)

CSIS (2)

**OTHER STAKEHOLDERS CONSULTED TO BE SENT COMMS MATERIALS
ON DAY OF TABLING**

FPT Cyber-crime working group

CACP Law amendments and Lawfully authorized electronic surveillance committee

**Telecommunications Service Providers: Yahoo, Mobile Satellite Ventures, Alberta
Supernet, FCI Broadband, Vonage**

Interception Solution Providers: Aqsacom, Detica, Spectronic

**Privacy Advocates: Privacy Commissioner of Ontario, Privacy Commissioner of
Alberta, Info & Privacy Commissioner of BC, New Brunswick Ombudsman,
BC Civil Liberties Association, Computer Professionals for Social Responsibility,
National Privacy Coalition, Priva Terra, Data Privacy Partners, Universite de Montreal,
Faculte de droit, UQAM, Commission d'accès a l'information, Ligue des droits et
libertés, BC Public Interest Advocacy Centre, Muslim Young Women's Association,
Committee for Racial Justice, BC Teachers Association, Law Society of British
Columbia, Manitoba Association for Rights and Liberties, Vancouver Community
Network, Telecommunities Canada**

Privacy Protections in TALEA:

A Comparison with Lawful Intercept Legislation in Other Western Countries

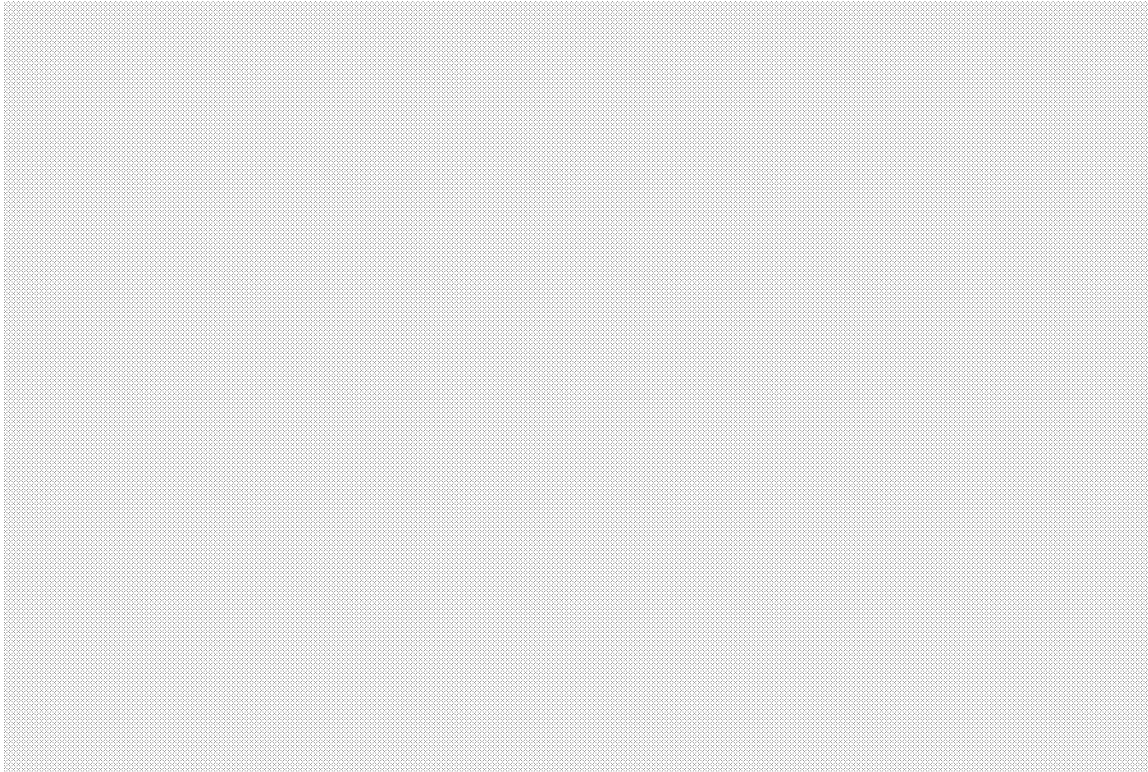
As the privacy protections established in TALEA relate to information handling practices of the public sector (including law enforcement and national security agencies) they are governed by, for example, the *Privacy Act* and other legislations that govern such bodies. In light of Industry Canada's mandate to oversee private sector privacy, [REDACTED]

The following is a collection of information drawn from a broad environmental scan. Information sources are drawn from internal Industry Canada documents, the Library of Parliament¹, and civil liberties organizations².

¹ *Telecommunications and Lawful Access: II. The Legislative Situation in the United States, the United Kingdom and Australia*

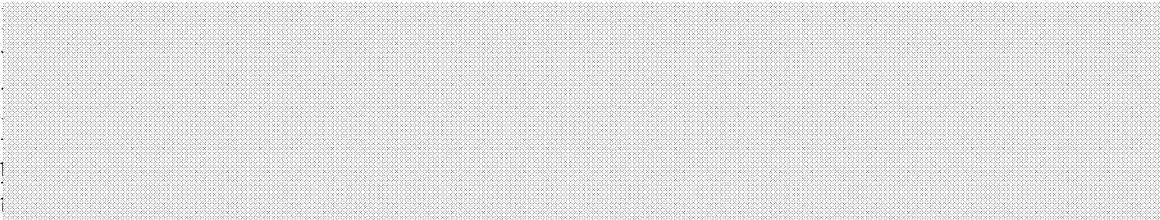
<http://www.parl.gc.ca/information/library/PRBpubs/prb0566-e.html#ukinterception>

² *Canadian government proposals for updating criminal laws and facilitating law enforcement in the electronic age* <http://www.cippic.ca/en/projects-cases/lawful-access/>



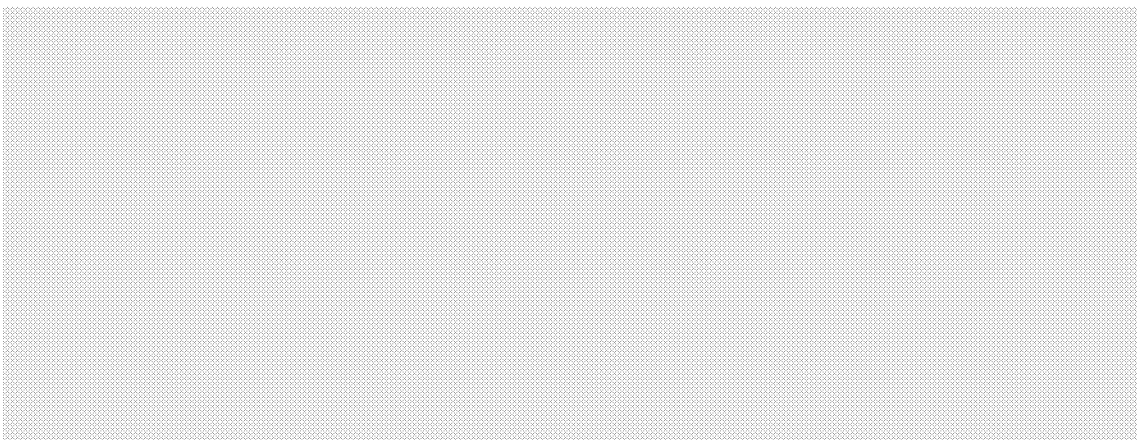
**Access to subscriber information:
Comparison between Canada US, UK, and Australia**

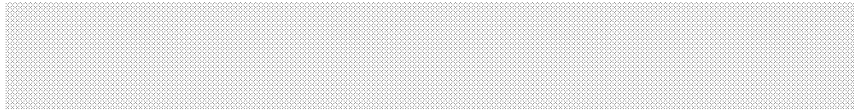
TALEA and CALEA (US)



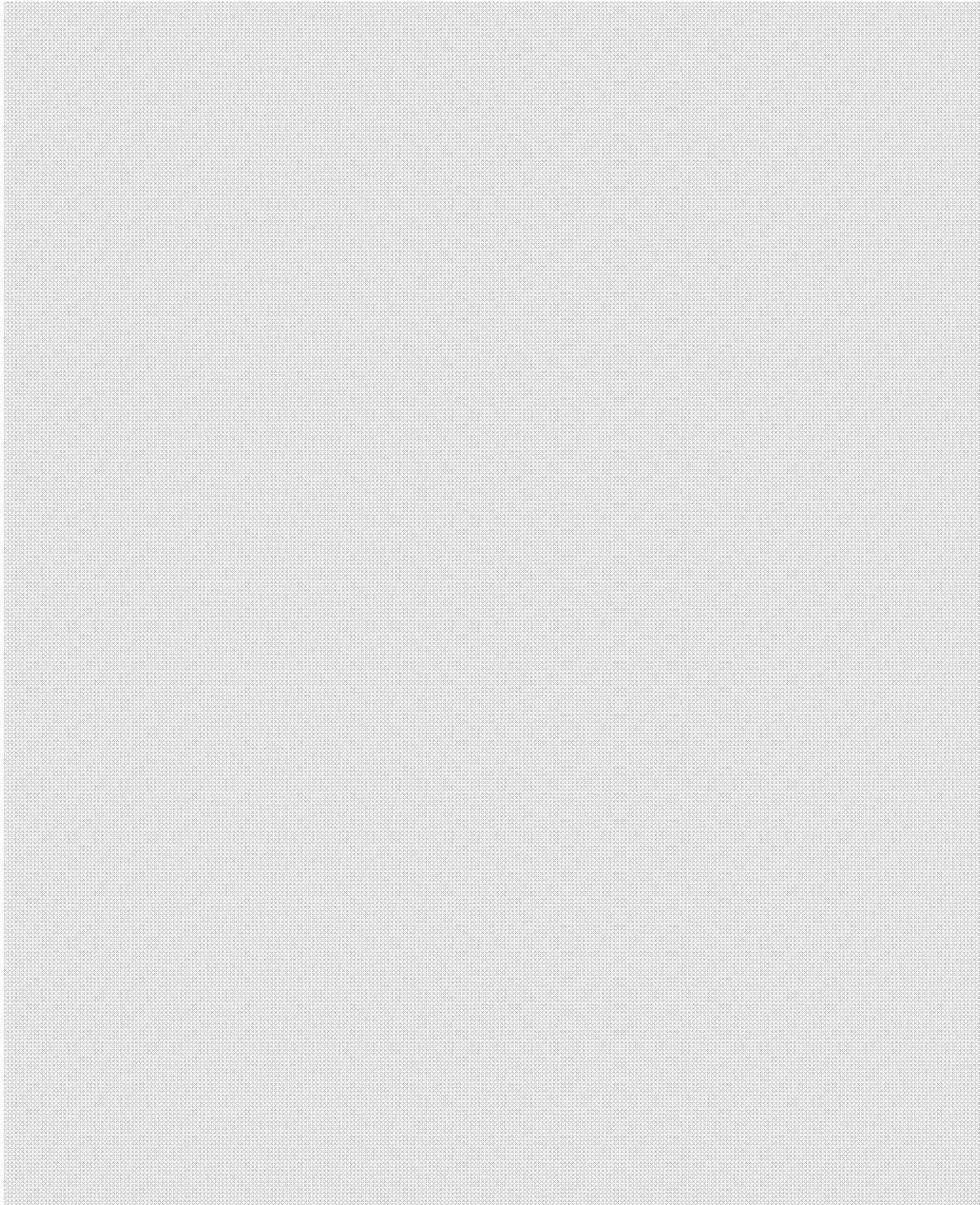
TALEA and RIPA (UK)

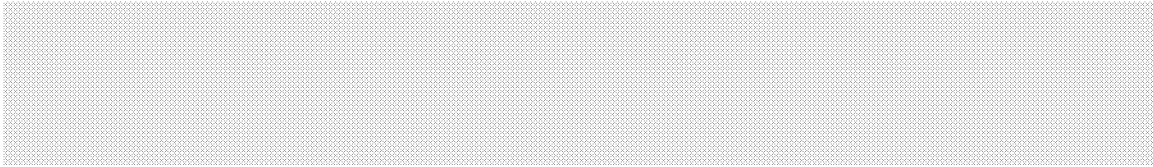
Storage of Transmission Data





Comparison with the Request for Information Under TALEA





Tariff rates for hook-up in other countries

However, for your information we include brief analysis from the U.K., Australia and New Zealand.

United States (1995)

Communications Assistance for Law Enforcement Act (CALEA),

In the U.S, hook-up fees vary widely. A hook-up to a network that is CALEA compliant costs law enforcement on average \$2,200, with some carriers charging as low as \$250 and others charging as high as \$3100. However, these costs might be inflated because investigators from the U.S. justice department are unable to determine if the carriers are passing capital costs on to law enforcement. TSP fees are also inconsistent charging different prices to different law enforcement agencies and differing by state.

We must note that pre-CALEA network upgrades were paid for by the FBI which was granted \$500 million for modifying systems installed or deployed prior to the coming into affect of CALEA on January 1, 1995.

United Kingdom (2000)

Regulation of Investigatory Powers Act (RIPA)

Any Communication Service Provider, such as a public telecommunications operator, postal carrier, Internet service provider or international simple voice resale provider is covered by RIPA. The cost burden on the telecoms industry of implementing the new measures has been substantial. RIPA imposes a duty on the Secretary of State to ensure that a service provider receives a "fair contribution" towards the cost of complying with an interception warrant or maintaining intercept capability.

A sum of £20 million was earmarked for communications provider support for the three years from 2001 to 2004 in connection with broader RIPA obligations, of which £14 million was spent in the first year. Further consultations are taking place between the Government, industry and the TAB on the precise costs to the industry of complying.

Australia (1979)

Telecommunications (Interception) Act

Telecommunications interception legislation is “designed to be technology-neutral and applies to any form of communication - voice, fax, images or data - passing over a telecommunications system. Specifically, Part 15 of the Telecommunications Act 1997 obligates carriage service providers (inc. ISPs) to ensure that their network is able to intercept a communication passing over it in accordance with a warrant issued under the Telecommunications (Interception) Act 1979.

For telecommunications carriers, the Bill stipulates that they must meet the costs of developing, installing and maintaining interception and delivery capabilities. However, carriers are still paid for what we would define as “Hook-Up”. According to the Australian Attorney General, total costs of interception per warrant ranges from AUS \$4,700 to \$22,953 of which “Hook-up” fees are included. As of October 22nd, 2007 \$1.16 AUS = \$1.00 CDN.

New Zealand 2004

Telecommunications Interception Capability Act.

In November 2004, New Zealand passed the *Telecommunications (Interception Capability) Act*. It requires network operators to ensure an interception capability of telecommunications networks and services.

Costs

The government will pay \$3M towards the provision of interception capability for existing fixed and mobile voice networks to be implemented within 18 months from the date the legislation is enacted.

ISPs will have to pay for the cost of upgrading their Internet and email services.

ISPs have been given five years to implement the changes needed to meet the requirements of the new law.

Information directly regarding “Hook-up” in NZ wasn’t available.

LISTE DES ADMs - LAWFUL ACCESS (2007-09-20)

Mr. Brian Saunders

Assistant Deputy Attorney General
Federal Prosecution Service
Department of Justice
284 Wellington Street, Room 2119
Ottawa, Ontario K1A 0H8

Brian.saunders@justice.gc.ca (957-4756)

(Francine Lance : 957-4757)

Assistant Commissioner Bruce Rogerson

Director
Technical Operations Directorate
RCMP
1426 St-Joseph Blvd
Gloucester, Ontario K1A 0R2

Carole.routhier@rcmp-grc.gc.ca

(Carole Routhier : 993-1619)

Rennie Marcoux

Assistant Secretary to the Cabinet
Privy Council Office
Security and Intelligence
59, Sparks Street, room 307B
Ottawa, Ontario K1A 0A3
(957-5386)

rmarcoux@pco-bco.gc.ca

(Sylvie Forcier : sforcier@pco-bcp.gc.ca (957-5386))

Scott Broughton

A/Senior Assistant Deputy Minister
Public Safety Canada
Office of SADM
269 Laurier Avenue West, Room 17A-1400
Ottawa, Ontario K1A 0P8
(991-2820)

Anne-Marie Doupagne (991-2819)

Anne-marie.doupagne@ps-sp.gc.ca

Ron Parker

Visiting Senior Assistant Deputy Minister, Industry Canada
Strategic Policy
235 Queen Street
1019A, East Tower
Ottawa, Ontario
K1A 0H5

Julie Malboeuf
(613) 947-3023

Mr. Michael Devaney

DG, Policy and Communications
Communications Security Establishment
719 Heron Road
Ottawa, Ontario K1A 0K2

michael.devaney@CSE-CST.GC.CA;
991-7140

tammy.varin@cse-cst.gc.ca (991-7254)

Mr. Ted Flanigan

Assistant Director Intelligence
Canadian Security Intelligence Service
1941 Ogilvie Road
Gloucester, Ontario K1J 1B7

flanigant@smtp.gc.ca (842-1487)

(Brigitte Henrie: 842-1210 ou Christine Warias 231-0652)

Michael M. Binder

Assistant Deputy Minister, Industry Canada
Spectrum, Information Technologies
And Telecommunications
300, Slater Street
Jean Edmonds Tower North, room 2035B, Floor 20
Ottawa, Ontario K1A 0C8

St-Jacques.Janet@ic.gc.ca
(Janet St-Jacques: 998-0368)

Ms. Sheridan Scott

Commissioner of Competition
Industry Canada
Competition Bureau
Place du Portagem Phase I, Floor 21, Zone 4
50 Victoria Street
Hull, Québec K1A 0C9

Diotte.Suzanne@cb-bc.gc.ca
(997-5300)

Donald K. Piragoff

Senior Assistant Deputy Minister
Department of Justice Canada
284 Wellington Street, EMB-50195
Ottawa, Ontario K1A 0H8

Chantal Pelchat (957-4726)

Lawful Access Privacy Consultations
Justice Canada

March

Monday	Tuesday	Wednesday	Thursday	Friday	Sat/Sun
	1	2	3	4	5/6
	8				12/13
			17	18	19/20
21	22	23		25 HOLIDAY	26/27
28 HOLIDAY	29 Ottawa: Canadian Bar Association & Assc. Of University Teachers ½ day (T)	30	31		

Notes

- Roundtable meetings will be held in a conference room in the hotel for both Montreal and Vancouver. A block of rooms at both hotels has been held for those who will be staying at the hotel.
- All meetings with Privacy Commissioner Offices will be held at their facilities (addresses indicated above).
- Ottawa roundtable to be held at Justice Canada.

Hotel Information

Montreal March 10th:

Hyatt Regency

1255 rue Jeanne-Mance

Phone : 514-982-1234

<http://montrealregency.hyatt.com/flash/hyattweb.swf>

Victoria March 13th:

Suggested hotel:

Victoria Marriott Inner Harbour

728 Humboldt Street

Phone : 250-480-3800

<http://marriott.com/property/propertypage.mi?marshaCode=YYJMC>

Vancouver March 14th & 15th∗:

The Westin Bayshore

1601 Bayshore Drive

Phone: 604-682-3377

www.westinbayshore.com

Edmonton March 16th:

Suggested hotel:

Courtyard Edmonton

One Thornton Court, 99 Street and Jasper Avenue

Phone: 780-423-9999

<http://marriott.com/property/propertypage.mi?marshaCode=YEGCY>

Comments on the Proposed *Modernization of Investigative Techniques Act*
(August 2006)

1. INTRODUCTION

ITAC, the Canadian Chamber, CAIP and the CWTA,¹ four leading Canadian industry associations, offer the following thoughts on the potential reintroduction of what was Bill C-74, the *Modernization of Investigative Techniques Act* (MITA). We represent a broad range of telecommunication service providers (TSPs) and equipment manufacturers, and our members collectively provide the overwhelming majority of residential and business telecommunication connections in Canada (wireline, wireless and internet services).

Our members have a long history of cooperation with Canada's law-enforcement and national-security agencies (LEAs) and of facilitating lawful access to electronic communications – subject to appropriate legal process and judicial oversight. The associations are therefore supportive of what we understand to be the basic objective that underpins MITA – to maintain LEAs' ability to lawfully intercept communications by ensuring that it covers all TSPs and new communication technologies as they are developed.

Recognising the overarching societal interest in public safety and security, the associations' members must at the same time carefully balance their desire for good corporate citizenship with the rights and expectations of their customers and the realities of their businesses. We are strongly of the view that the cost of providing a lawful-access regime for the benefit of society should be borne by society as a whole and not just by consumers of telecom services. Furthermore, we would not want to see legislative initiatives that would detract from the privacy protections that Canadian TSPs are bound to maintain and on which their customers and clients have come to depend.

We note that there seems to be general acceptance of the following key points:

- The current framework for lawful access in Canada is generally working well, with broad cooperation from the ICT industry. LEAs are able to effect lawful interception, even for newer services – though not using standardised technology provided by TSPs.
- New legislation is needed to extend requirements equally to all TSPs and all technologies so as to ensure universal availability of lawful-access capability and to extend LEA access to basic subscriber identification information from traditional telephony to newer technologies.

¹ The Information Technology Association of Canada, the Canadian Chamber of Commerce, the Canadian Association of Internet Providers and the Canadian Wireless Telecommunications Association, respectively.

- Lawful-access requirements are not intended to have a detrimental impact on Canadians – by stifling innovation, by unduly impeding or delaying the roll-out of new products and services (including the extension of voice and broadband service to underserved communities) or by compromising personal privacy unreasonably.
- New legislation is not intended to download additional costs of policing from government and law enforcement to TSPs and their customers, recognising that TSPs, as a subset of the larger business community, already have a unique and disproportionate burden and responsibility for lawful access.
- New legislation is not intended to alter the scope or frequency of electronic surveillance in Canada, or the current balance between personal privacy and public safety.

However, the associations have serious concerns about MITA as drafted and introduced previously, and would be unable to support it in that form. Essentially, MITA as introduced is at odds with the above key points in terms of the following: mandated infrastructure capability that may not yet be supported by manufacturers and recognised standards; a lack of compensation for TSPs' operational costs; and a "transition" period that amounts to mandated retrofit.

2. ASSOCIATION PROPOSALS

2.1 Mandated Capability before Standards

2.1.1 The Problem

A key concern with MITA, as previously introduced, is that it required TSPs to meet specified operational requirements without regard to the availability of commercial standards-based equipment and software that would meet those requirements.

While commercial equipment and software that meets most of the operational requirements is available from manufacturers for established wireline services, it is not always available for newer and developing services. This is in part because the operational requirements set out in MITA do not yet apply to as broad a spectrum of telecom technologies in other countries, including the United States, so there is little market incentive to build in capabilities.

The associations do not object to Canadian TSPs shouldering the additional incremental cost when acquiring new equipment when intercept-capable, standards-based equipment and software is commercially available. However, we have serious concerns about the application of lawful-access capability requirements before standards-based equipment and software is readily available. This is because the costs of custom-built lawful-access solutions could

be significant and the time required to develop such solutions could produce a significant impediment to productivity and speed-to-market.

Furthermore, the need for the custom solutions is likely to be short-lived as standards-based commercial solutions become available within a short period of time. This could have a number of negative implications for TSPs, including stranded investments or the need to continue to expand and service an expensive custom-built solution due to incompatibility between the jerry-built solution and the later commercial standards-based solution.

MITA attempted to address this issue by providing for Ministerial orders suspending, for particular TSPs, the obligation to comply with certain operational requirements while the TSPs built out alternative solutions. In addition, time-limited Governor-in-Council exemptions would be available for certain classes of TSPs; however, each application for relief would be entirely discretionary, potentially time-consuming, costly and procedurally daunting. Moreover, such a scheme will prove to be extremely inefficient and taxing for TSPs and the Minister and Cabinet during the early years of implementation, when commercial capability is much less likely to be available for newer services and technologies.

It should be emphasised that a gap between the application of MITA's infrastructure capability requirements and the commercial availability of standards-based transmission apparatus may not be limited to an initial transition period following legislation being passed and the coalescing of international standards for lawful intercept. Indeed, should there be future uncertainties with respect to lawful-access capability requirements in other jurisdictions – particularly the United States – standards-based, intercept-capable equipment may not be available with respect to future services or technologies that Canadian service providers may want to introduce.

Situations might arise where new products or services are available for use in the US without any imposed lawful-access requirement, but where Canadian consumers are prevented from using the services until Ministerial forbearance has been applied for, processed and granted. This would be bad for TSPs, for Canadian consumers and business, and for Canada's productivity, innovation and competitiveness.

2.1.2 The Solution

The associations submit that a more appropriate approach would be to create two types of infrastructure obligations for TSPs:

- one where standards-based, lawful-access capable equipment is commercially available
- one where such equipment is not yet available.

In the first scenario, TSPs would be required to purchase new transmission apparatus with lawful-access capability, consistent with the regime contemplated in MITA, and would absorb the incremental cost of doing so. In the second, the associations submit that the Government should determine whether, where and to what extent lawful-access capability is required, and then require affected TSPs to develop and implement customised solutions – on the understanding that the TSPs will be compensated for doing so.

The approach would be similar to that contained in the United Kingdom's *Regulation of Investigatory Powers Act* (RIPA), which allows the Secretary of State to impose obligations on TSPs to maintain a reasonable intercept capability, but requires the Secretary of State to ensure that the TSPs in question receive fair compensation for the costs of providing that capability.² In this way, infrastructure deployment is efficiently targeted to services, service areas or service providers of interest to LEAs, and service providers do not bear a disproportionate burden in funding lawful-access capability.

Whereas RIPA does not contain a general requirement to provide lawful-access capability and includes infrastructure capability requirements that are triggered only by order of the Secretary of State, the associations would accept the general obligation for lawful-access capability contained in section 10 of MITA. However, the obligation would be limited to circumstances where commercially available standards-based transmission apparatus is available. In order to deal with circumstances where such apparatus is not available, we propose that MITA be amended to include provisions, similar to the RIPA provisions discussed above, empowering the Minister of Public Safety to order specified TSPs to implement specified lawful-access capability in specified areas – with compensation to the TSP coming from funds provided by Parliament for the purpose. A similar power currently exists in section 15 of MITA, but applies only to extraordinary infrastructure capability that the Minister may require beyond the standing obligations elsewhere in MITA.

The question of when standards-based transmission apparatus is commercially available, and the appropriate compensation for infrastructure capability built pursuant to Ministerial order, would be decided by a joint government / industry technical committee, similar to one proposed by the Department of Public Safety and Emergency Preparedness (PSEPC) during industry consultations prior to the introduction of Bill C-74 or to the Technical Advisory Board created by section 13 of RIPA.

New Canadian legislation could require TSPs to provide notice of pending service introductions (with strict confidentiality protections in view of the highly competitive nature of the industry), and could also provide the Minister with a power to require TSPs to estimate the cost and time required to implement a customised solution, with such estimates to be provided within a specified period

² *Regulation of Investigatory Powers Act 2000* (U.K.), 2000, c. 23, ss. 12 to 14.

(e.g., 90 days). In this way, the Minister could balance efficiency and industry productivity against investigative needs and cost requirements, thereby minimising any gaps in the availability of lawful-access capability for services that warrant such cost and effort. The associations understand that this is much the way that LEAs currently assess cases and assign resources and funding; MITA should require nothing less.

2.2 No Compensation for Operational Costs

2.2.1 The Problem

The associations are very concerned by the fact that MITA is entirely silent on the question of compensation for operational costs, notwithstanding that the topic is currently a significant point of dispute between certain LEAs and TSPs, wherein the agencies have refused to pay the service providers in question for a range of services.

Generally, TSPs receive compensation from LEAs to perform many warranted or otherwise mandated services. In our view, such compensation continues to be appropriate, particularly in light of the growing number of interceptions and other warranted actions. MITA does not prohibit TSPs charging LEAs for providing subscriber identification information on request without a warrant. TSPs are private businesses, with mandates wholly unrelated to policing and unconnected to criminal activity, yet TSPs and their subscribers are increasingly called upon to engage significant costs associated with receiving and processing all sorts of lawful-access orders. In so doing, TSPs furnish telecom-transport and technical-support services that in all fairness must be compensated.

2.2.2 The Solution

The associations recommend that MITA be amended so as to include a scheme that would provide reasonable compensation to TSPs for carrying out activities relating to the warranted interception of private communications and the statute-mandated provision of TSP subscriber information. In our view, these requirements apply uniquely to TSPs and, particularly in the case of interceptions, require unique technical and operational advice and assistance. Such compensation would be within the purview of MITA, as opposed to more general forms of search-warrant activity and legislation.

The associations note that precedents for such compensation arrangements exist in other jurisdictions. Along with compensation for the provision of lawful-access capability mandated by the UK Secretary of State, RIPA also provides that the UK government ensure that there be arrangements to ensure that TSPs receive a fair contribution to the costs of providing assistance in respect of individual warrants.³ The American wiretap statute provides explicitly for

³ *Regulation of Investigatory Powers Act 2000* (U.K.), 2000, c. 23, s. 14.

reasonable compensation to those furnishing facilities or technical assistance in connection with a wiretap.⁴ In Australia, the *Telecommunications Act* requires TSPs to provide assistance to LEAs in connection with wiretaps, among other things, on the basis that the TSP neither profits from, nor bears the cost of, giving that assistance.⁵

As noted above, the associations understand that Parliament, the provinces and municipalities currently provide, through LEA budgets, sums to cover the costs of interceptions of private communications. Indeed, payments are routinely made by most LEAs for both the development of infrastructure capability and the provision of warranted and other assistance. We submit that such funding should continue to be available to compensate TSPs for carrying out wiretap orders and responding to mandated requests for subscriber information pursuant to section 17 of MITA.

2.3 Transition Period amounts to Mandated Retrofit

2.3.1 The Problem

The associations are strongly of the view that a transition period is necessary in order to accommodate the long lead times required to plan and build out networks and network components. Network elements that were planned 18 months earlier cannot be made to comply immediately with operational requirements that come into force two days before the new components are turned up.

In discussions with PSEPC staff prior to the introduction of MITA, the associations were led to believe that there would be an initial transition period, following the coming into force of the legislation, to allow TSPs to incorporate the newly mandated operational requirements into their construction programs. While a 12-month transition period was provided for in section 58 of MITA, at the end of the transition period TSPs would have to retrofit the equipment built or installed during the transition period in order to meet the operational capabilities. Frankly, this amounts to no transition period at all, since retrofitting solutions will always be more cumbersome and expensive than building in capability at the outset.

2.3.2 The Solution

The associations recommend that the transition period be amended so that the requirements of section 10 come into force 12 months after the rest of the Act is proclaimed in force. Transmission apparatus installed during this 12-month period would be grandfathered as fully compliant with MITA, unless it is

⁴ *Electronic Communications Privacy Act*, 18 U.S.C. §2518(4).

⁵ *Telecommunications Act 1997* (Aus.), s. 314.

subsequently upgraded in a way that would trigger lawful-access capability requirements pursuant to other provisions of the legislation.

3. CONCLUDING REMARKS

The associations will be unable to support MITA if it is reintroduced in its current form. The proposals offered above are narrowly targeted to address our most significant concerns so as to minimise the impact on the existing framework of MITA and thus the need for revision. Although each was discussed at a conceptual level only, we will be pleased to discuss these proposals in detail or to propose specific wording to capture these proposals in any new bill.



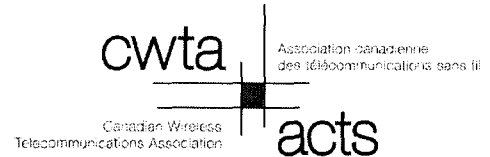
INFORMATION TECHNOLOGY
ASSOCIATION OF CANADA

ASSOCIATION CANADIENNE DE LA
TECHNOLOGIE DE L'INFORMATION



THE CANADIAN
CHAMBER
OF COMMERCE

LA CHAMBRE
DE COMMERCE
DU CANADA



August 25, 2006

Ms Suzanne Hurtubise
Deputy Minister
Public Safety and Emergency Preparedness Canada
340 Laurier Avenue West
Ottawa, ON K1A 0P8

Dear Deputy Minister:

re: Legislation regarding Lawful Interception of Telecommunications

Canada's telecommunication industry has for many years cooperated with law-enforcement and national-security agencies by facilitating lawful interception of telecom services for investigations relating to crime and national security.

However, as noted in our March 10, 2006 letter to the Minister, our industry does not want to see new lawful-interception requirements that will hamper the development and introduction of new services and technologies, increase costs and diminish the competitiveness of Canadian telecom service providers.

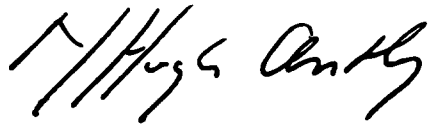
We have had productive meetings with staff from your department in recent weeks. The attached paper restates our fundamental concerns and proposes conceptual solutions as requested. We will be very pleased to meet to discuss these issues in more detail.

Sincerely,

Bernard A. Courtois
President and CEO
Information Technology Association of Canada

David Elder
Chair, Lawful Access Committee
Canadian Association of Internet Providers

Peter Barnes
President
Canadian Wireless Telecommunications Association
000235

A handwritten signature in black ink, reading "Nancy Hughes Anthony". The signature is written in a cursive style with a large, stylized initial "N".

Nancy Hughes Anthony
President and CEO
Canadian Chamber of Commerce

Comments on the Proposed *Modernization of Investigative Techniques Act*
(August 2006)

1. INTRODUCTION

ITAC, the Canadian Chamber, CAIP and the CWTA,¹ four leading Canadian industry associations, offer the following thoughts on the potential reintroduction of what was Bill C-74, the *Modernization of Investigative Techniques Act* (MITA). We represent a broad range of telecommunication service providers (TSPs) and equipment manufacturers, and our members collectively provide the overwhelming majority of residential and business telecommunication connections in Canada (wireline, wireless and internet services).

Our members have a long history of cooperation with Canada's law-enforcement and national-security agencies (LEAs) and of facilitating lawful access to electronic communications – subject to appropriate legal process and judicial oversight. The associations are therefore supportive of what we understand to be the basic objective that underpins MITA – to maintain LEAs' ability to lawfully intercept communications by ensuring that it covers all TSPs and new communication technologies as they are developed.

Recognising the overarching societal interest in public safety and security, the associations' members must at the same time carefully balance their desire for good corporate citizenship with the rights and expectations of their customers and the realities of their businesses. We are strongly of the view that the cost of providing a lawful-access regime for the benefit of society should be borne by society as a whole and not just by consumers of telecom services. Furthermore, we would not want to see legislative initiatives that would detract from the privacy protections that Canadian TSPs are bound to maintain and on which their customers and clients have come to depend.

We note that there seems to be general acceptance of the following key points:

- The current framework for lawful access in Canada is generally working well, with broad cooperation from the ICT industry. LEAs are able to effect lawful interception, even for newer services – though not using standardised technology provided by TSPs.
- New legislation is needed to extend requirements equally to all TSPs and all technologies so as to ensure universal availability of lawful-access capability and to extend LEA access to basic subscriber identification information from traditional telephony to newer technologies.

¹ The Information Technology Association of Canada, the Canadian Chamber of Commerce, the Canadian Association of Internet Providers and the Canadian Wireless Telecommunications Association, respectively.

- Lawful-access requirements are not intended to have a detrimental impact on Canadians – by stifling innovation, by unduly impeding or delaying the roll-out of new products and services (including the extension of voice and broadband service to underserved communities) or by compromising personal privacy unreasonably.
- New legislation is not intended to download additional costs of policing from government and law enforcement to TSPs and their customers, recognising that TSPs, as a subset of the larger business community, already have a unique and disproportionate burden and responsibility for lawful access.
- New legislation is not intended to alter the scope or frequency of electronic surveillance in Canada, or the current balance between personal privacy and public safety.

However, the associations have serious concerns about MITA as drafted and introduced previously, and would be unable to support it in that form. Essentially, MITA as introduced is at odds with the above key points in terms of the following: mandated infrastructure capability that may not yet be supported by manufacturers and recognised standards; a lack of compensation for TSPs' operational costs; and a "transition" period that amounts to mandated retrofit.

2. ASSOCIATION PROPOSALS

2.1 Mandated Capability before Standards

2.1.1 The Problem

A key concern with MITA, as previously introduced, is that it required TSPs to meet specified operational requirements without regard to the availability of commercial standards-based equipment and software that would meet those requirements.

While commercial equipment and software that meets most of the operational requirements is available from manufacturers for established wireline services, it is not always available for newer and developing services. This is in part because the operational requirements set out in MITA do not yet apply to as broad a spectrum of telecom technologies in other countries, including the United States, so there is little market incentive to build in capabilities.

The associations do not object to Canadian TSPs shouldering the additional incremental cost when acquiring new equipment when intercept-capable, standards-based equipment and software is commercially available. However, we have serious concerns about the application of lawful-access capability requirements before standards-based equipment and software is readily available. This is because the costs of custom-built lawful-access solutions could

be significant and the time required to develop such solutions could produce a significant impediment to productivity and speed-to-market.

Furthermore, the need for the custom solutions is likely to be short-lived as standards-based commercial solutions become available within a short period of time. This could have a number of negative implications for TSPs, including stranded investments or the need to continue to expand and service an expensive custom-built solution due to incompatibility between the jerry-built solution and the later commercial standards-based solution.

MITA attempted to address this issue by providing for Ministerial orders suspending, for particular TSPs, the obligation to comply with certain operational requirements while the TSPs built out alternative solutions. In addition, time-limited Governor-in-Council exemptions would be available for certain classes of TSPs; however, each application for relief would be entirely discretionary, potentially time-consuming, costly and procedurally daunting. Moreover, such a scheme will prove to be extremely inefficient and taxing for TSPs and the Minister and Cabinet during the early years of implementation, when commercial capability is much less likely to be available for newer services and technologies.

It should be emphasised that a gap between the application of MITA's infrastructure capability requirements and the commercial availability of standards-based transmission apparatus may not be limited to an initial transition period following legislation being passed and the coalescing of international standards for lawful intercept. Indeed, should there be future uncertainties with respect to lawful-access capability requirements in other jurisdictions – particularly the United States – standards-based, intercept-capable equipment may not be available with respect to future services or technologies that Canadian service providers may want to introduce.

Situations might arise where new products or services are available for use in the US without any imposed lawful-access requirement, but where Canadian consumers are prevented from using the services until Ministerial forbearance has been applied for, processed and granted. This would be bad for TSPs, for Canadian consumers and business, and for Canada's productivity, innovation and competitiveness.

2.1.2 The Solution

The associations submit that a more appropriate approach would be to create two types of infrastructure obligations for TSPs:

- one where standards-based, lawful-access capable equipment is commercially available
- one where such equipment is not yet available.

In the first scenario, TSPs would be required to purchase new transmission apparatus with lawful-access capability, consistent with the regime contemplated in MITA, and would absorb the incremental cost of doing so. In the second, the associations submit that the Government should determine whether, where and to what extent lawful-access capability is required, and then require affected TSPs to develop and implement customised solutions – on the understanding that the TSPs will be compensated for doing so.

The approach would be similar to that contained in the United Kingdom's *Regulation of Investigatory Powers Act* (RIPA), which allows the Secretary of State to impose obligations on TSPs to maintain a reasonable intercept capability, but requires the Secretary of State to ensure that the TSPs in question receive fair compensation for the costs of providing that capability.² In this way, infrastructure deployment is efficiently targeted to services, service areas or service providers of interest to LEAs, and service providers do not bear a disproportionate burden in funding lawful-access capability.

Whereas RIPA does not contain a general requirement to provide lawful-access capability and includes infrastructure capability requirements that are triggered only by order of the Secretary of State, the associations would accept the general obligation for lawful-access capability contained in section 10 of MITA. However, the obligation would be limited to circumstances where commercially available standards-based transmission apparatus is available. In order to deal with circumstances where such apparatus is not available, we propose that MITA be amended to include provisions, similar to the RIPA provisions discussed above, empowering the Minister of Public Safety to order specified TSPs to implement specified lawful-access capability in specified areas – with compensation to the TSP coming from funds provided by Parliament for the purpose. A similar power currently exists in section 15 of MITA, but applies only to extraordinary infrastructure capability that the Minister may require beyond the standing obligations elsewhere in MITA.

The question of when standards-based transmission apparatus is commercially available, and the appropriate compensation for infrastructure capability built pursuant to Ministerial order, would be decided by a joint government / industry technical committee, similar to one proposed by the Department of Public Safety and Emergency Preparedness (PSEPC) during industry consultations prior to the introduction of Bill C-74 or to the Technical Advisory Board created by section 13 of RIPA.

New Canadian legislation could require TSPs to provide notice of pending service introductions (with strict confidentiality protections in view of the highly competitive nature of the industry), and could also provide the Minister with a power to require TSPs to estimate the cost and time required to implement a customised solution, with such estimates to be provided within a specified period

² *Regulation of Investigatory Powers Act 2000* (U.K.), 2000, c. 23, ss. 12 to 14.

(e.g., 90 days). In this way, the Minister could balance efficiency and industry productivity against investigative needs and cost requirements, thereby minimising any gaps in the availability of lawful-access capability for services that warrant such cost and effort. The associations understand that this is much the way that LEAs currently assess cases and assign resources and funding; MITA should require nothing less.

2.2 No Compensation for Operational Costs

2.2.1 The Problem

The associations are very concerned by the fact that MITA is entirely silent on the question of compensation for operational costs, notwithstanding that the topic is currently a significant point of dispute between certain LEAs and TSPs, wherein the agencies have refused to pay the service providers in question for a range of services.

Generally, TSPs receive compensation from LEAs to perform many warranted or otherwise mandated services. In our view, such compensation continues to be appropriate, particularly in light of the growing number of interceptions and other warranted actions. MITA does not prohibit TSPs charging LEAs for providing subscriber identification information on request without a warrant. TSPs are private businesses, with mandates wholly unrelated to policing and unconnected to criminal activity, yet TSPs and their subscribers are increasingly called upon to engage significant costs associated with receiving and processing all sorts of lawful-access orders. In so doing, TSPs furnish telecom-transport and technical-support services that in all fairness must be compensated.

2.2.2 The Solution

The associations recommend that MITA be amended so as to include a scheme that would provide reasonable compensation to TSPs for carrying out activities relating to the warranted interception of private communications and the statute-mandated provision of TSP subscriber information. In our view, these requirements apply uniquely to TSPs and, particularly in the case of interceptions, require unique technical and operational advice and assistance. Such compensation would be within the purview of MITA, as opposed to more general forms of search-warrant activity and legislation.

The associations note that precedents for such compensation arrangements exist in other jurisdictions. Along with compensation for the provision of lawful-access capability mandated by the UK Secretary of State, RIPA also provides that the UK government ensure that there be arrangements to ensure that TSPs receive a fair contribution to the costs of providing assistance in respect of individual warrants.³ The American wiretap statute provides explicitly for

³ *Regulation of Investigatory Powers Act 2000* (U.K.), 2000, c. 23, s. 14.

reasonable compensation to those furnishing facilities or technical assistance in connection with a wiretap.⁴ In Australia, the *Telecommunications Act* requires TSPs to provide assistance to LEAs in connection with wiretaps, among other things, on the basis that the TSP neither profits from, nor bears the cost of, giving that assistance.⁵

As noted above, the associations understand that Parliament, the provinces and municipalities currently provide, through LEA budgets, sums to cover the costs of interceptions of private communications. Indeed, payments are routinely made by most LEAs for both the development of infrastructure capability and the provision of warranted and other assistance. We submit that such funding should continue to be available to compensate TSPs for carrying out wiretap orders and responding to mandated requests for subscriber information pursuant to section 17 of MITA.

2.3 Transition Period amounts to Mandated Retrofit

2.3.1 The Problem

The associations are strongly of the view that a transition period is necessary in order to accommodate the long lead times required to plan and build out networks and network components. Network elements that were planned 18 months earlier cannot be made to comply immediately with operational requirements that come into force two days before the new components are turned up.

In discussions with PSEPC staff prior to the introduction of MITA, the associations were led to believe that there would be an initial transition period, following the coming into force of the legislation, to allow TSPs to incorporate the newly mandated operational requirements into their construction programs. While a 12-month transition period was provided for in section 58 of MITA, at the end of the transition period TSPs would have to retrofit the equipment built or installed during the transition period in order to meet the operational capabilities. Frankly, this amounts to no transition period at all, since retrofitting solutions will always be more cumbersome and expensive than building in capability at the outset.

2.3.2 The Solution

The associations recommend that the transition period be amended so that the requirements of section 10 come into force 12 months after the rest of the Act is proclaimed in force. Transmission apparatus installed during this 12-month period would be grandfathered as fully compliant with MITA, unless it is

⁴ *Electronic Communications Privacy Act*, 18 U.S.C. §2518(4).

⁵ *Telecommunications Act 1997* (Aus.), s. 314.

subsequently upgraded in a way that would trigger lawful-access capability requirements pursuant to other provisions of the legislation.

3. CONCLUDING REMARKS

The associations will be unable to support MITA if it is reintroduced in its current form. The proposals offered above are narrowly targeted to address our most significant concerns so as to minimise the impact on the existing framework of MITA and thus the need for revision. Although each was discussed at a conceptual level only, we will be pleased to discuss these proposals in detail or to propose specific wording to capture these proposals in any new bill.

**Consultations de suivi sur l'accès licite:
rencontre de suivi avec la société civile
– Montréal, 11 mars 2005 –**

Le contexte de la rencontre

La rencontre a été organisée à l'initiative du ministère de la Justice du Canada, en collaboration avec d'autres organismes publics fédéraux d'une part et d'Option consommateurs, d'autre part. Option consommateurs avait notamment pour mandat d'inviter les représentants de la société civile dans la région de Montréal susceptibles d'être intéressés par les problématiques soulevées à participer à la rencontre. En tout, zz invitations ont été envoyées¹. En tout, zz (8?) représentants de la société civile ont participé à la rencontre.

Cette consultation fait partie d'un processus entamé en août 2002 et visant à obtenir l'éclairage de divers milieux canadiens à l'égard de modifications susceptibles d'être effectuées à l'égard de diverses lois fédérales pour tenir compte des progrès technologiques en matière de télécommunications et d'engagements internationaux que le Canada pourrait ratifier. Une première rencontre avec la société civile avait eu lieu en novembre 2002 à Montréal. En tout, le gouvernement du Canada a reçu plus de trois cents (300) mémoires dans le cadre de ce processus.

Bien que le calendrier parlementaire relatif à l'adoption de ces modifications législatives demeure inconnu, la vice-première ministre a indiqué à l'automne 2004 que le gouvernement comptait agir «le plus vite possible».

On procédera ici à une synthèse des commentaires recueillis au cours de la rencontre du 11 mars 2005. On ne reprendra évidemment pas intégralement le contenu des présentations des divers représentants gouvernementaux, puisqu'on le retrouve dans les documents distribués aux participants à la rencontre². L'ordre du jour proposé a été suivi dans l'ensemble et le contenu transmis aux participants correspondait de près au contenu de ces documents.

1- Propositions de modifications au *Code criminel*

¹ On trouvera ci-joint la liste des invitations effectuées. Elle inclut notamment des organismes communautaires, les milieux universitaires, des entreprises, les milieux professionnels et les milieux syndicaux.

² zz adresse web de ces documents.

A- Le contexte général

Si l'Internet comporte évidemment des avantages considérables pour la société, ce réseau fournit aussi aux criminels de nouvelles occasions d'escroquer les gens et les nouvelles méthodes de télécommunications leur permettent également de communiquer entre eux à des fins criminelles (ou terroristes) par de nouvelles méthodes. Les dispositions législatives actuellement en vigueur ne permettent pas nécessairement de réprimer les nouvelles formes de criminalité, comme la transmission de virus, le vol d'identité, le refus de service distribué ou l'appâtage; elles n'autorisent pas non plus les autorités chargées du respect des lois à intercepter toutes ces formes de communications. La dernière mise à jour du *Code criminel* dans ce secteur, qui évolue très rapidement, a été effectuée en 1997.

Parmi les problèmes précis qui peuvent être évoqués, outre la définition de nouvelles infractions et les pouvoirs d'interception, figurent les difficultés liées à la préservation d'éléments de preuve qui peuvent être très volatiles et les défis associés aux demandes d'assistance mutuelle entre corps policiers. Des problématiques telles que celles soulevées par la conservation à l'étranger de documents informatiques canadiens requièrent aussi l'attention du législateur³. Actuellement, ce sont surtout les dispositions relatives à des questions de procédure qui requièrent une mise à jour.

Cette première présentation n'a pas donné lieu à des commentaires particuliers.

B- La modernisation du libellé

La mise à jour de la législation soulève d'abord un certain nombre de difficultés d'ordre général. Par exemple, les définitions de la notion de «télécommunication», utilisée dans plusieurs lois, devraient être harmonisées. Dans le contexte de cette modernisation, les moyens de défense existants seraient pour l'essentiel maintenus et adaptés eux aussi⁴.

Les données relatives à l'aiguillage des communications posent des difficultés particulières, dans la mesure notamment où elles peuvent inclure des éléments analogues au «contenu» d'une communication; la distinction entre données de transmission et contenu, qui peuvent être assujetties à des règles différentes en matière d'interception, devra donc faire l'objet d'une attention particulière. On pourra s'inspirer à cet égard de libellés législatifs utilisés à l'étranger, comme par exemple au Royaume-Uni.

La discussion s'est alors engagée au sein du groupe. Pour un participant, «qui ne dit mot ne consent pas» et le recours à un concept comme l'expectative raisonnable de vie privée comporte cette difficulté que plus la police peut fouiller, plus cette expectative se réduit et donc plus les droits de la personne font l'objet d'une érosion. On invite le législateur à retenir des définitions comportant un contenu objectif, comme la notion de

³ On a par exemple noté que les dossiers informatiques de l'*Ontario Health Insurance Program* sont conservés en Ohio, aux États-Unis.

⁴ On a entre autres donné l'exemple de l'article 191 C.Cr., relatif à la possession de dispositifs d'interception.

«renseignements personnels». Un désaccord s'est manifesté à l'égard du caractère objectif du critère d'«expectative raisonnable». On a aussi signalé avec étonnement qu'alors que la Cour suprême des États-Unis a jugé que le recours policier aux techniques de thermographie était inacceptable, la Cour suprême du Canada a pour sa part conclu récemment que de telles pratiques n'étaient pas indûment attentatoires aux droits fondamentaux⁵.

On a ensuite tenu une pause.

C- Les ordonnances de communication et de localisation

La révision des dispositions législatives relatives aux ordonnances de communication pose des défis importants. On doit d'une part mettre au point un langage technologiquement neutre. Il faut aussi distinguer les données de transmission des contenus. La difficulté à cet égard devient flagrante quand on envisage des pratiques comme l'utilisation du clavier téléphonique pour naviguer dans un système de télébanque ou pour obtenir une prescription, par exemple. Ces distinctions sont importantes dans la mesure où des ordonnances pourront être obtenues par les autorités chargées de l'application de la loi dans la mesure où elles ont des «motifs raisonnables de *souçonner*» ou des «motifs raisonnables de *croire*» qu'une infraction pourrait être commise, selon le cas.

Un participant a fait observer que l'automatisation des habitudes de vie et diverses pratiques commerciales exposent beaucoup plus d'opérations à l'interception; il serait paradoxal que cette évolution sociale rende à elle seule la vie des citoyens plus «transparente» pour les autorités⁶. Une participante a noté que les autorités doivent pouvoir commencer leur enquête quelque part et que la barre ne doit donc pas être placée trop haut, sans quoi on causera la paralysie des pouvoirs policiers; il ne lui paraissait toutefois pas nécessaire de procéder à des modifications significatives au *Code criminel* pour atteindre les objectifs recherchés. Mais, s'est interrogé un autre participant, pourrait-on aller jusqu'à mettre une puce de localisation dans le sac à main d'une personne dont on soupçonne qu'elle pourrait enfreindre la loi?

On a d'autre part noté les difficultés liées au visa d'un mandat émis dans une autre province par les autorités locales: il semblerait que le visa soit souvent accordé de manière routinière, sans analyse. On envisage par conséquent d'abolir cette formalité, qui paraît inutile. Un participant a toutefois signalé qu'il faudrait ici poser autrement la question: à quelle fin a-t-on décidé qu'un visa local serait requis? Et si un besoin légitime existe toujours, ce n'est pas parce que le processus actuel n'est pas appliqué correctement qu'il faut abolir tout contrôle. Une participante a noté dans ce contexte que l'administration de la justice pénale relève de la compétence provinciale, et qu'il est donc normal qu'un mandat soit visé localement; des modifications au régime légal des juge de

⁵ *Kyllo v. United States*, ZZ; ZZ.

⁶ L'utilisation d'une carte de crédit ou de débit, par exemple, permet de localiser assez précisément son détenteur (ou un usurpateur, ce qui pose également des difficultés d'un autre ordre).

paix devraient par ailleurs accroître leur indépendance à l'avenir. Un participant s'est demandé si on cherchait au fond ici à accommoder les autorités états-uniennes, ce à quoi on lui a répondu par la négative.

C- Les ordonnances de conservation

Les ordonnances de conservation visent à éviter que des éléments de preuve ne soient détruits avant qu'un mandat permettant de les obtenir ne soit émis. Il a été précisé qu'elles ne pourraient avoir pour effet d'obliger un tiers à conserver des renseignements qu'il ne détient pas dans le cours ordinaire de ses affaires: un fournisseur d'accès Internet qui ne détient pas certains types de données ne pourrait donc être contraint à les recueillir à la seule fin de se conformer à une ordonnance. On a également confirmé que la personne visée n'est normalement pas informée de l'émission d'une ordonnance de conservation; un participant a fait observer que cette personne pouvait toutefois subir un dommage important en raison de l'émission de l'ordonnance (surtout s'il s'avère qu'elle n'a rien à se reprocher), et ce à son insu.

Un autre participant s'est inquiété du risque qu'on étende la portée d'obligations de délation, qui existent par exemple en matière de pornographie juvénile.

D- Les ordonnances d'assistance

La notion d'ordonnance d'assistance est fondée sur le devoir de *common law* du citoyen d'aider l'État à faire son travail. Ces ordonnances posent toutefois certaines difficultés. D'une part, la personne qui fournit son assistance a-t-elle droit à une indemnisation de la part de l'État? Les tribunaux canadiens lui accordent à l'occasion un dédommagement quand la contribution requise excédait les bornes d'une aide raisonnable. D'autre part, la personne qui ne se conforme pas à une demande d'assistance qui serait déraisonnable encourt le risque d'une condamnation pénale onéreuse (en vertu de l'art. 487.017 C.Cr.). Un participant a fait observer que le tiers requis de fournir son assistance pourrait fort bien se trouver en conflit entre l'obligation légale d'assister, d'une part, et des obligations contractuelles de ne pas poser les actes requis par l'ordonnance d'assistance, d'autre part; on a rappelé à cet égard l'existence de l'art. 25 C.Cr.

E- L'interception des courriels

L'obtention des courriels pose des difficultés inusitées. Par exemple, s'agit-il d'une interception, ou d'une saisie? Comment qualifie-t-on un message texte envoyé par téléphonie cellulaire et qui s'apparente par sa teneur à un courriel? Le statut du courriel varia-t-il selon la phase de son existence, i.e. selon qu'il est en cours de transmission, stocké par un fournisseur de service, reçu par le destinataire...? Compte tenu de la nature du courriel, quelle est la portée de l'expectative raisonnable de vie privée à son égard?

On envisage dans les solutions proposées le recours à une notion d'«interception» qui fait appel à l'obtention «de façon simultanée» d'une communication sans le consentement d'une partie. Un participant a noté que le recours à une telle notion de simultanéité

pourrait causer des problèmes pratiques, compte tenu de la nature du processus de transmission des courriels.

F- L'entraide juridique

On a évoqué la révision de la *Loi sur l'entraide juridique en matière criminelle* à la lumière de l'éventuelle ratification de la *Convention sur la cybercriminalité*. La problématique n'a pas évoqué de commentaires particuliers, sinon des réserves sur la pertinence que le Canada ratifie cette convention.

On a ensuite pris une pause pour le lunch.

2- Propositions de modifications à la *Loi sur la concurrence*

Quoique les pouvoirs dont il dispose existent depuis 1985 et aient toujours été maintenus par la Cour suprême, le Bureau de la concurrence constate maintenant que son arsenal de moyens d'interception et de saisie ne correspond plus à l'évolution des pratiques illicites qu'il est chargé de réprimer et qu'il doit fréquemment tenter de recourir à la collaboration des forces policières pour mener ses enquêtes. Au plan constitutionnel, les questions dont le Bureau est chargé peuvent par ailleurs ne pas relever toutes du droit criminel et certaines donnent lieu à des procédures dites «civiles», et non strictement pénales. On voudrait donc à la fois modifier le libellé de certains textes d'incrimination afin qu'ils visent, par exemple, «toutes formes de télécommunication», sans limitation.

Un participant a requis des clarifications quant à l'extension qu'on voudrait donner à la portée de l'article 52.1 de la *Loi sur la concurrence*. Un autre voulait savoir pourquoi on désirait modifier cette loi, ce qui a donné lieu à un rappel des conclusions de l'arrêt *Hunter c. Southam*. Ce dernier participant a par ailleurs souligné l'importance de la distinction entre les affaires civiles et pénales, les premières ne devant pas nécessairement donner lieu à une extension aussi importante des pouvoirs d'enquête.

3- Propositions relatives à la sécurité publique et aux interceptions

On a ensuite abordé des questions reliées principalement aux interceptions de télécommunications. En raison de l'évolution technologique, les services policiers ne peuvent souvent plus procéder seuls aux interceptions: ils requièrent inévitablement le concours des fournisseurs de services de télécommunication pour pouvoir capter les messages. Les besoins policiers en cette matière soulèvent deux enjeux: le coût que peut imposer la collaboration avec les services policiers aux fournisseurs de services, et les modifications que ces derniers pourraient devoir apporter à leurs pratiques.

Des discussions ont présentement cours avec les fournisseurs de services de télécommunications afin de conclure des accords relatifs aux coûts. Il paraît par ailleurs admis que la législation ne requerrait pas les fournisseurs de modifier leurs pratiques d'affaire ou leurs installations à la seule fin de faciliter des interceptions. Des exceptions aux obligations de collaboration seraient par ailleurs aménagées pour les exploitants de réseaux de communication privés, comme les universités, par exemple.

Par ailleurs, les normes techniques auxquelles devraient se conformer les fournisseurs de service seraient rendues publiques. Ces normes s'appliqueraient au fur et à mesure que les fournisseurs remplaceraient leurs équipements et leurs processus, et non à toutes les opérations des fournisseurs dès leur mise en vigueur.

Quant aux questions relatives à la cryptographie, les autorités ont pris acte qu'elles avaient perdu il y a déjà quelques années la bataille relative à la divulgation systématique des clés.

On a d'autre part noté au cours de la discussion que les personnes faisant l'objet d'une interception n'en seraient le plus souvent pas informées, même *a posteriori*. On s'est également étonné que les discussions relatives aux normes techniques ou à d'autres questions soient tenues dans un forum non officiel entre le gouvernement et l'industrie, excluant la société civile, et qu'elles échappent par conséquent au processus démocratique.

À l'égard des coûts qui devront progressivement être encourus pour mettre en place les capacités d'interception souhaitées, des représentants gouvernementaux ont reconnu qu'ils seraient «substantiels», mais qu'ils ne constitueraient néanmoins qu'un pourcentage congru des investissements de toute manière requis afin de moderniser constamment les installations des fournisseurs. De l'avis de certains participants, les coûts pourraient fort bien s'avérer en fait très considérables, tout en produisant peu de résultats réels parce que les criminels s'installeront tout bonnement dans d'autres juridictions. On a évoqué un alignement des orientations canadiennes vers celles des autorités états-uniennes, plutôt que vers celles des autorités européennes. On a aussi noté que les autorités canadiennes semblent traiter indistinctement de terrorisme, de criminalité, de pédophilie, au détriment de la liberté d'expression et des règles qui visaient jusqu'à maintenant à l'exonération de responsabilité du transporteur à l'égard de la teneur des communications acheminées.

Les représentants des autorités ont précisé qu'elles n'entendent pas ici modifier la définition des infractions elles-mêmes et qu'il importe qu'elles puissent accomplir leur mandat, en partageant équitablement les coûts avec l'industrie et dans le cadre d'une étroite supervision par les mécanismes de contrôle politiques, administratifs et judiciaires existants. On a aussi noté que les mécanismes d'interception sont rentables au plan économique et induisent moins de risques que le recours à des agents doubles, par exemple.

4- Propositions relatives aux renseignements sur les abonnés

La notion de «renseignements sur les abonnés» vise des éléments comme leur nom, leur adresse, leur numéro de téléphone (y compris les numéros confidentiels) ou leurs adresses Internet (URL et smtp notamment). Les autorités établissent une distinction entre ces données et d'autres en matière d'«expectative raisonnable de vie privée», parce qu'elles n'auraient pas trait à l'intimité des individus. Les pratiques relatives à l'obtention de tels renseignements sont actuellement totalement variables et difficilement prévisibles.

Les propositions qui sont formulées ne requerraient pas que les fournisseurs modifient leurs pratiques d'affaires et donc qu'ils recueillent ou ne conservent plus de renseignements qu'ils n'en obtiennent déjà.

Un débat s'est engagé sur la nomenclature des infractions pouvant donner lieu à l'émission d'ordonnances de divulgation de ces renseignements, compte tenu que les modalités d'obtention seraient moins onéreuses que celles relatives à un mandat de perquisition, par exemple. On a précisé dans ce cadre qu'un policier devrait fournir une attestation sous sa signature à l'égard des motifs d'obtention d'une ordonnance et qu'une attestation mensongère constituerait un faux.

La rencontre s'est terminée par un bref échange plus général où des participants ont fait valoir l'importance d'une participation citoyenne démocratique aux débats relatifs à ces questions et ont souligné que l'action policière a pour objet de défendre la cohésion des liens sociaux, qu'elles ne doivent donc pas menacer par des pratiques abusives. L'accent a été mis sur le respect d'un critère de nécessité à l'égard de l'intrusion dans la vie privée des citoyens. Les représentants des autorités ont souligné que le processus en cours visait justement à assurer la transparence requise dans le processus et à rechercher l'équilibre entre les divers intérêts en présence.

On a enfin noté que les intéressés sont invités à faire état de commentaires écrits à l'égard des propositions formulées au cours des prochaines semaines, quoiqu'on ne sache pas quand un projet de loi visant à adopter ces diverses mesures sera déposé.

La rencontre s'est conclue vers 16:15h.

Date: August 25, 2006

Draft / Ébauche



Final



MEDIA LINES / INFOCAPSULES

Bill C-74 Modernizing Investigative Techniques to Maintain Public Safety and National Security (MITA)

ISSUE / ENJEU

Modernizing investigative techniques to maintain public safety and national security

KEY MESSAGES / MESSAGES CLÉS

- Industry Canada fully supports the goal of improving lawful access capabilities to prevent, investigate and prosecute serious offences, organized crime and threats to national security, particularly in light of new technologies.
- Industry Canada is pleased with the contribution of key stakeholders to improve the proposed legislation and welcomes Parliament's review.
- Parliament will review the proposed legislation to ensure it achieves a careful balance between enhancements to public safety and national security, while safeguarding the privacy of Canadians and sustaining innovation and the competitiveness of Canadian industries.

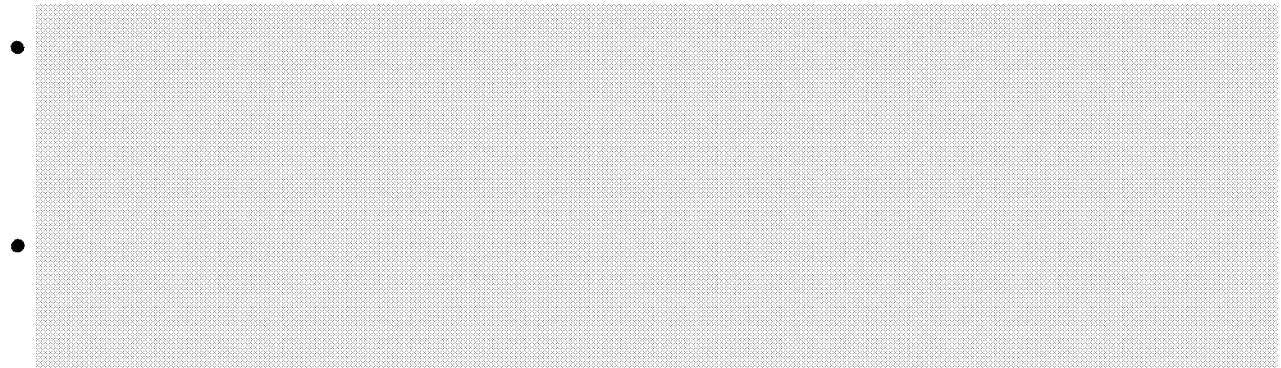
SPOKESPERSON / PORTE-PAROLE

Media Relations Office / Bureau des relations avec les médias — (613) 943-2502

s.21(1)(b)

BACKGROUND / CONTEXTE

- Public Safety and Emergency Preparedness Canada is the lead department for this file.
- *Modernizing Investigative Techniques to Maintain Public Safety and National Security* (also known as *Lawful Access*) was tabled on Tuesday, November 15, 2005, by then Deputy Prime Minister and Minister of Public Safety and Emergency Preparedness and co-signed by the Minister of Industry. It died on the Order Paper.

**PREPARATION AND APPROVALS / PRÉPARATION ET APPROBATION**

Prepared by / Préparé par	Key Contact / Personne-ressource	Approved by / Approuvé par	Date
Hélène Vigeant CMB Senior Communications Advisor for Spectrum, Information Technologies and Telecommunications (613) 947-6331	Louis LePage A/Director Industry Framework Policy (613) 998-4367 André Leduc ECOM (613) 990-4958	TO DETERMINE WHO IS APPROVING Len St-Aubin Acting DG, DGTP (613) 998-4341	August 25, 2006

PROJET DE LOI C-416*Loi sur la modernisation des techniques d'enquête (LMTE)*

Marlene Jennings, députée libérale et porte-parole en matière de justice

Position du Ministère :

Le ministère de l'Industrie appuie un examen du projet de loi présenté au Parlement ainsi qu'une version COMPLÈTE ET FINALE du règlement y afférent.

Le ministère appuie l'objectif qui consiste à maintenir et à améliorer les capacités techniques pour les interceptions des télécommunications autorisées par la loi. L'amélioration des capacités ne doit pas porter indûment atteinte à la vie privée des particuliers ni entraver sérieusement la prestation de services de télécommunication aux Canadiens et la compétitivité de l'industrie.

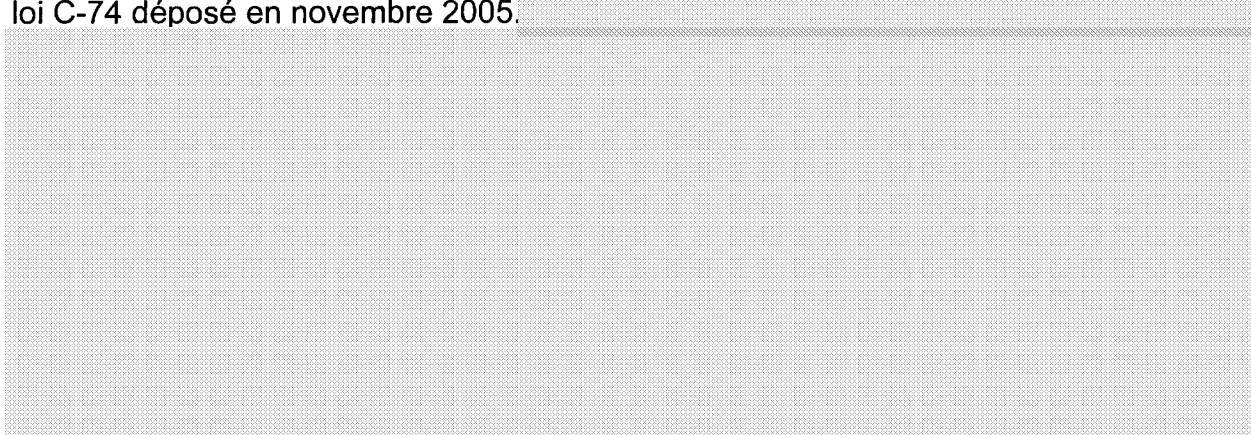
Le ministre de la Sécurité publique devrait être responsable de la réponse du gouvernement au projet de loi C-416. La réponse pourrait notamment consister à appuyer le projet de loi C-416 tel quel et le projet de loi C-416 sous réserve de modifications ou à déposer l'ébauche de la *Loi sur l'assistance technique pour l'application de la loi / Technical Assistance to Law Enforcement Act (TALEA)*

Résumé factuel du projet de loi

Le projet de loi a pour objet d'améliorer les capacités techniques visant à procéder à l'interception des télécommunications en vertu des pouvoirs légaux existants sans toutefois porter indûment atteinte à la vie privée des particuliers ou entraver sérieusement la prestation de services de télécommunication aux Canadiens et la compétitivité de l'industrie.

Brève évaluation

Nous notons que le projet de loi C-416 est vu comme étant identique au projet de loi C-74 déposé en novembre 2005.



BILL C-416**Modernization of Investigative Techniques Act (MITA)****Marlene Jennings, Liberal MP and Justice Critic**Department's Position:

Industry Canada supports a review of the proposed Bill in Parliament along with a COMPLETE AND FINAL version of the associated Regulations.

Industry Canada supports the goal to maintain and improve capabilities for lawful interception of telecommunications. However, improved capabilities must not unreasonably impair the privacy or the provision of telecommunications to Canadians and the industry's competitiveness.

The Minister of Public Safety should have leadership for a Governmental response to Bill C-416. Most likely options include the support of Bill C-416, the support of Bill C-416 with amendments, or the tabling of the draft Technical Assistance to Law Enforcement Act (TALEA)/Loi sur l'assistance technique pour l'application de la loi which is the current government version of the bill.

Factual Summary of the Bill:

The Bill aims to improve the technical capabilities to carry-out the interception of telecommunications under existing lawful authorities while not unreasonably impairing the privacy or the provision of telecommunications to Canadians and the industry's competitiveness.

Brief Assessment:

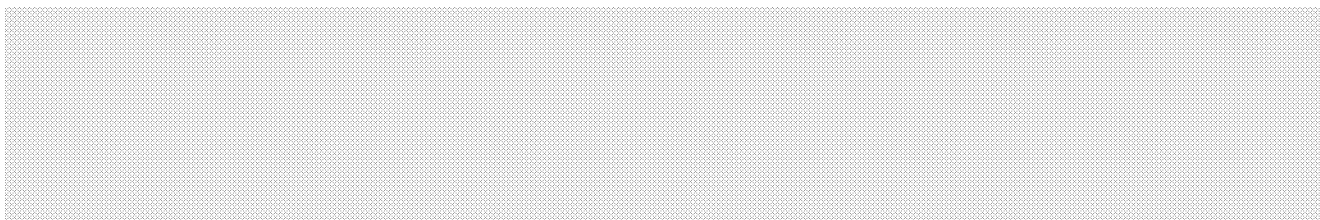
We note that Bill C-461 is reported as identical to Bill C-74 tabled in November 2005.



s.21(1)(a)

s.21(1)(b)

SECRET



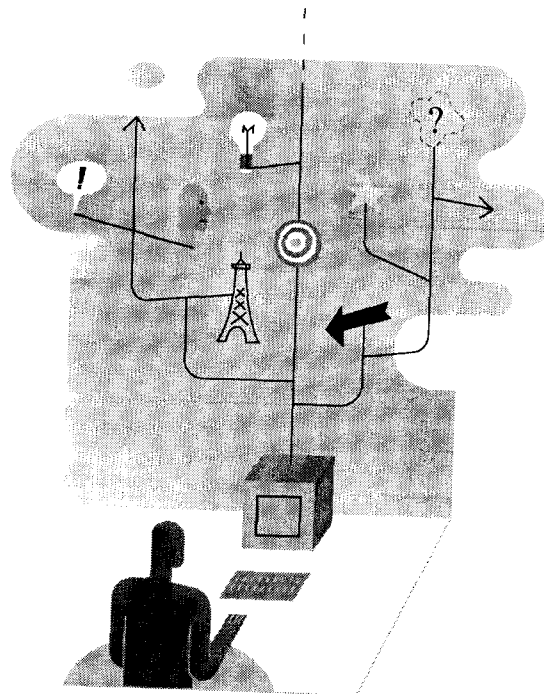
ITAC

INFORMATION TECHNOLOGY
ASSOCIATION OF CANADA

ACTI

ASSOCIATION CANADIENNE
DE LA TECHNOLOGIE DE L'INFORMATION

Customer Name and Address Consultation



October 2007

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

© 2007 Information Technology Association of Canada

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Dr. Avner Levin
Director, Privacy and Cyber Crime Institute
Chair, Law and Business Department

October 8, 2007

Ms. Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security

Re: CNA Information Consultation

Dear Ms. Clairmont,

Thank you for inviting me to participate in the CNA Information Consultation. I am pleased to provide my comments on the Consultation Document in this letter. These comments are based significantly on the public reassurances made by Minister Day during recent media appearances, in which the Minister appears to have stated that the proposed legislation will not provide Law Enforcement Agencies (LEAs) with the power to lawfully access CNA information without a warrant. I support the Minister's position and view it as at the right approach to take at the present time.

It is important to note that my support for the Minister's present position is not based on a "knee-jerk" reaction to the Consultation Document. I agree wholeheartedly with the concerns of LEAs about increased terrorism and national security risks, as well as their concerns about cyber-crime in general. I agree as well to the need to ensure the cooperation of TSPs in emergency situations, such as recent well-publicized cyber child molestation incidents.

Unfortunately, I have yet to see empirical evidence of the difficulties that LEAs claim to have experienced in obtaining CNA information from TSPs. I would urge Public Safety to request such information from LEAs. It would be useful for LEA supporters to have at their disposal statistics that detail investigations that have been hampered by the judicial oversight currently in place, especially since privacy advocates voice the concern that warrants are often issued with little scrutiny of LEAs. Police investigators often state in public appearances the technological difficulties of a modern cyber forensic investigation, or the legal difficulties of international investigation and extradition treaties, which do indeed need to be streamlined to allow for efficient and swift procedures. I do not recall however a case in which LEAs identified a TSP that refused to cooperate (voluntarily) in a situation where an individual was threatened or molested, or where cyber-criminals, let alone terrorists, were not brought to justice because of the reluctance of the judicial system to issue warrants.

I believe that the Canadian public would strongly support access to CNA information in emergency situations, and generally without judicial warrants, if presented with such unequivocal statistical evidence. I also believe that the Canadian public and the present Federal Government are quite sensible in retaining the present judicial oversight mechanism in place as long as there is no such demonstrated need. I would be happy to continue and participate in a CNA consultation on the merits of an administrative model once LEAs have made the empirical case for their requests.

Sincerely,

(-)

Avner Levin

Alicia Wanless.txt

International Perspectives International Perspectives
Ms. Lynda Clairmont Associate Assistant Deputy Minister Emergency Management &
National Security

Public Safety Canada

16C, 269 Laurier Ave. W.,
Ottawa ON, K1A 0P8

Thursday, October 4th, 2007

Dear Ms. Clairmont,

Thank you for the invitation to participate in consultations regarding an important security measure, Lawful Access. I have avidly followed the subject both in Canada and internationally for a number of years and am happy to provide some thoughts on current endeavours to implement a Canadian Lawful Access measure.

Lawful Access legislation is a critical security measure. The ability to intercept communications enables law enforcement agencies to gain valuable insight and evidence with which to build cases around suspected criminals. Many countries have opted to update existing or implement new measures as a result of the widespread use of emerging communication technologies. Canada is one of a few countries that has not enacted separate regulations around Lawful Access (LA). The chief reason why such important legislation has to date not been enacted stems from a failure to build consensus among key stakeholders as to what shape such LA legislation and, ultimately, regulations should take.

Central to this absence of consensus has been a lack of disclosure of statistics around past and current uses of wiretapping and release of Customer Name and Address (CNA) information as investigative tools. In fact, little to no statistical data covering any aspect of LA, as it is currently used, that can support the need to implement a new bill or enhance existing provisions has been publicly provided. This lack of disclosure not only renders draft LA measures baseless, but also causes much distrust among key stakeholders outside of the law enforcement realm.

Collecting and analysing data around the current use of LA provides a solid understanding for how a new security measure should be created. Such statistics indicate how useful the measure has been to date, which in turn can quantify exactly what sort of resources should be allocated to enhancing provisions and what those enhancements should be. For example, statistics might indicate that due to emerging communications technologies the costs associated with enhancing

□
2

interception capabilities on some internet-based services is far greater than the benefits to society of such enhancements. As a result, resources may be better allocated to developing innovative policing methods that answer the changing realities of modern investigations. Conversely, statistics may indicate that the measure is exceptionally useful and provide a clear picture of how best to move forward based on legitimate evidence acceptable to all key stakeholders.

Without statistics around the current use of LA as a basis for provision enhancements any attempts to push through a new measure will certainly be met with widespread disapproval. It is conceivable that basing a security measure, such as LA, on the requests of law enforcement in the absence of supporting data can negatively impact the image of respect held by police among the Canadian public. This is especially true at a time when one of our federal law enforcement agencies is increasingly scrutinised as a result of corruption allegations

while no one doubts the need of law enforcement in Canada, it must be remembered that even those entrusted to uphold the law require oversight. The human factor must be taken into account. It should not be inconceivable that there remains the potential for abuse of a tool such as wiretapping. Such abuse might include corrupt police officers abetting criminal organizations or a frustrated investigator abusing poorly regulated privileges to gather information on a suspect where official channels have failed. Providing statistics around the current use of LA in Canada would assist in quelling such concerns held by privacy advocates. Furthermore the provision of statistics would help engage privacy advocates in creating a measure that benefits society.

From a security perspective, introducing a security measure without supporting data risks the stability of the entire governing system. As the stability of our society depends upon the symbiosis between civil society and law enforcement, any actions that jeopardise the necessary respect for and co-operation with Canadian police among the general public have the potential to negatively impact the wider system in the long run. Despite a seeming readiness among Canadians to forgo certain civil liberties in the name of security, measures enacted without foundation risk eroding such faith in leadership, particularly when those measures strengthen the perception of enhanced security as opposed to actually making Canada more secure. Indeed, Canadians have proven to have a surprisingly low threshold for tolerating security measures that fail to protect the best interests of citizens (consider, for example, the incident in Grand Manan, New Brunswick during the summer of 2006.) Using a scientific approach in implementing new LA legislation will

Alicia Wanless.txt

ensure that the respect currently enjoyed by law enforcement in Canada is continued well into the future.

Statistics on the current use of LA also provide much needed insight as to what the technical scope of enhancements to existing provisions should be. The costs of implementing new

www.internationalperspectives.org • 1.416.556.8717 •
info@internationalperspectives.org

□
3

technology to comply with LA legislation can be considerable. Supporting data can assist in developing regulations and parameters for enhancing LA provisions thus providing a well-defined scope and targets which industry can then meet. In the absence of supporting data and analysis, any plans to enhance existing LA provisions will be carried out blindly. After all, it is impossible to determine scope without first understanding what reasonable and efficient technical enhancements are actually needed. Without a clear, well-founded plan as to how LA enhancements will be carried out, it should be anticipated that industry would view attempts to pass a measure unfavourably.

Considering these different angles, I strongly recommend that basic information regarding the current use of LA be immediately collected and analysed before any further attempts at implementing a measure be carried out. At a minimum, the following information should be collected over an appropriate period (perhaps six (6) months or as long as required in a given sector), while at the same time preparing a basic framework for the new measure as incoming data indicates scope:

- The number of times wiretapping or requests for CNA information are being made, broken down by requesting organization as well as type of request;
 - whether the request for a warrant or CNA information was refused and why;
 - The nature of the crime or circumstance why such requests are being made;
 - Type of communication technology to be intercepted and whether or not the surveillance attempt was successful; &
 - Direct correlation as to the usefulness of the request with closing the investigation as well as prosecution of the target.
- To ensure the integrity of the data collected, both law enforcement agencies as well as counterparts inside of CSPs should be mandated to collect the above information. The data retention

Alicia Wanless.txt

process could be as simple as completing and submitting an official form, thus enabling an almost immediate implementation of the reporting mechanism.

A small committee of individuals, each representing a respective key stakeholder, should be set up at arm's length to analyse the data and put forth findings and recommendations for moving forward. Such a reporting process should continue on a permanent basis to ensure accountability of measures such as LA.

www.internationalperspectives.org • 1.416.556.8717 •
info@internationalperspectives.org

□
4

with a proper approach it is possible to enact a measure efficiently that protects civil liberties as well as facilitates law enforcement without over burdening industry. Such a balance, however, can only occur if the measure is based on supporting statistics and all perspectives are considered equally in the drafting of such a bill. I believe that the above recommendations will assist the government in achieving the necessary balance while also enacting an effective long-term measure.

Should you have any questions regarding the thoughts presented in this letter or need clarification, please do not hesitate in contacting me.

(Stamp comment
Signature Alicia Wanless
04/10/2007 2:57:18 PM
blank)
Sincerely,

Alicia Wanless
Executive Director

International Perspectives

1.416.556.8717
awanless@internationalperspectives.org

www.internationalperspectives.org • 1.416.556.8717 •
info@internationalperspectives.org

□

CUSTOMER NAME AND ADDRESS

CONSULTATIONS

Public Safety Canada

By: Canadian Resource Centre for Victims of Crime
October 10, 2007

□
Introduction

The Canadian Resource Centre for Victims of Crime (CRCVC) is a non-government, non-profit advocacy group for victims and survivors of violent crime. We provide direct assistance to victims across the country as well as advocate for more services and protections for victims and the public. We were pleased to receive an invitation from Public Safety Canada to participate in the consultation process regarding possible measures to address law enforcement and national security agencies' lawful access to customer name and address (CNA) information held by telecommunications service providers (TSPs).

As a non-government organization dedicated to ensuring the voice of victims and survivors is heard, we agree that the rights and freedoms guaranteed in the Canadian Charter of Rights and Freedoms must be protected. However, the protection of an individual's privacy cannot take precedence over the protection of the public from national security threats or the protection of children from sexual exploitation.

Canada is in no way immune to terrorist threats, as seen with the arrest of a Quebec man in connection with an online plot to bomb targets outside Canada on September 14, 2007. If not for the prompt response of the RCMP and other law enforcement groups, a serious incident may have occurred.

We have long advocated for increased protections for child victims; including those who may be sold, prostituted or used for child pornography. Our largest area of focus has been on advocating for increased resources for law enforcement to allow them to fully investigate and rescue children from sexual exploitation on the Internet.

As stated in the consultation document, law enforcement has repeatedly voiced their concerns about the difficulty in consistently obtaining basic CNA information in the course of their duties. Officials need prompt cooperation from TSPs in order to prevent threats to national security/public safety and to rescue abused children. It is our opinion that corporations should be

obligated to assist law enforcement (without a warrant), as any good citizen would, in preventing and investigating crime.

Customer Name and Address Consultations

Submitted by: Canadian Resource Centre for Victims of Crime

□
Our position

In 2000, the CRCVC sent a discussion paper to all Members of Parliament and Senators entitled "Child Sexual Exploitation and the Internet." We made 20 recommendations, including that legal requirements be imposed on Internet Service Providers (ISPs) to cooperate with law enforcement, the creation of a new offence of luring, raising the age of consent, creation of a national tip-line, etc. It is unfortunate that seven years later, law enforcement agencies still face challenges accessing basic CNA information.

The lack of explicit legislation in this area gives telecommunications companies the discretion to provide information to law enforcement when it is requested or to demand a court order before releasing any information at all, regardless of the situation at hand. This is problematic at any stage of an investigation, likely halting it or creating significant delays while documents to compel the information are sought. We should not have to reiterate the risk of delays in the context of preventing terrorism or rescuing children from sexual abuse. We believe the government should immediately amend section 7(3) of the Personal Information Protection and Electronic Documents Act (PIPEDA) to make it clear that 'lawful authority' does not require a warrant in order to ensure the police and national security agencies are granted CNA information.

We fully support the use of safeguards, as listed in the consultation document. In order to prevent abuses, for example, we support limits on who can have access to the information, limiting how it is used, and internal audits on the use of the powers, etc. We agree that lawful access to CNA information should not include the content of communications or the web sites an individual visited online unless a court order is issued.

Concerns of privacy advocates

The problem of child pornography on the Internet is getting worse, and despite the many successes of Canadian law enforcement, police are only able to scratch the surface. We applaud the continued, difficult work of police officers in sorting through tens of thousands of images of child pornography in order to catch the predators and stop the abuse of children. Their objectives are simple - arrest those who create, distribute and access child pornography and identify and

rescue those children who have already been harmed.

Some privacy advocates suggest, "Canadian law enforcement and national security agencies are looking for a quick and easy way to obtain access to the names, phone numbers, IP addresses, etc

Customer Name and Address Consultations

Submitted by: Canadian Resource Centre for Victims of Crime

□ of customers of Canadian telecommunications service providers. Quick and easy, in this context, means without the delay and paperwork involved in applying to a judge for a search warrant."¹ We urge officials to remember that police/national security officials seek this information in a number of contexts, including in the very beginning of investigations or as part of intelligence gathering. We submit that persons who come to the attention of law enforcement or national security agencies in the course of their investigative duties are 'persons of interest'. Their actions online have raised serious red flags. We do not believe that CNA information is sought when there is insufficient evidence to connect an individual to a crime so that a judge would not issue a warrant.

Law enforcement and national security agencies must act quickly when such 'persons of interest' come to their attention. There is not always ample time to obtain lawful authority in the form of a warrant. Immediate threats to national security and the sexual abuse of children must override the protection of anyone's personal information by PIPEDA.

We urge Public Safety officials to remember the privacy violations of the innocent children whose images are being traded like baseball cards every day for the sexual satisfaction of pedophiles and predators. There is no greater violation of privacy than having images and videos of someone raping you distributed around the world. We cannot allow these crimes to continue to be facilitated by private companies in Canada who provide broadband Internet access, virtual storage areas for abuse images and anonymous e-mail, and forums for pedophiles to support each other in the belief that having sex with children is not wrong.

Tom Copeland, head of the Canadian Association of Internet Providers, has stated that requiring a search warrant for police to get a suspect's name and address is "over-kill" and that information is not normally considered private. We agree, and would submit, that much of the "personal information" held by TSPs is already public information contained in most telephone directories.

We also submit that cooperation by TSPs on a case-by-case basis, which is what generally occurs now, is simply not good enough when it comes to the safety/protection of children

or threats to national security. Privacy advocates maintain that there must be court oversight in order to hand over personal information and that police investigations have not been hampered to date.

1 David T.S. Fraser, "Some necessary background information to the fuss over warrant-less access to Canadian personal information,"

15 September 2007.

<http://www.privacylawyer.ca/blog/2007/09/some-necessary-background-to-fuss-over.htm>

Customer Name and Address Consultations
Submitted by: Canadian Resource Centre for Victims of Crime

□ However, investigations have been hampered, as reported by many police officers during the Statutory Review of PIPEDA in 2006/2007. In our opinion, police do not and should not need a warrant to secure subscriber information or in any other circumstance except when dictated by Parliament.

Police do not need a warrant to check a license plate in order to identify the owner of a vehicle that is suspected of being involved in a crime. There are many examples where law enforcement has access to information that the average citizen does not. They have access to this information because they are tasked with preventing and investigating crime and they have an already well established legal obligation not to disclose the information that they obtain except within the course of their mandated duties.

The Problem

As PIPEDA currently exists, it requires the consent of the individual for all collection, use and disclosure of personal information, subject to a number of exceptions. "Personal information" includes any information about an identifiable individual. It is thus illegal for TSPs to disclose such information without consent.

What constitutes lawful authority is at question. Subsection 7(3)(c) of the legislation is where the confusion occurs, as it sets out provisions where an organization may disclose personal information without consent. The first condition is when it is in compliance with a subpoena, warrant or court order. The second stipulation for disclosure is in response to a request by a government institution that has the lawful authority to obtain the personal information for the purpose of enforcing a law, carrying out an investigation related to the enforcement of the law, or gathering intelligence for purposes of enforcing a law.²

It is the term lawful authority that is problematic. On December 18, 2006, the Privacy Commissioner wrote the CRCVC and stated that under section 7(3)(c.1)(ii), "the

decision to disclose the information rests with the organization...In other words, the disclosure is discretionary on the part of the organization." We submit, once again, that discretionary

2 Section 7(3)(c.1) states that an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is "made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs, (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or (iii) the disclosure is requested for the purpose of administering any law of Canada or a province;"

Customer Name and Address Consultations
Submitted by: Canadian Resource Centre for Victims of Crime

□ disclosure is simply unacceptable when it comes to public safety and the sexual exploitation of children.

CRCVC Recommendations

Given the confusion that exists regarding lawful authority and the hesitation of some TSPs to comply with law enforcement requests, we recommend (at the minimum) that section 7(3) be amended to make it clear 'lawful authority' does not mean a warrant is required. Lawful access to CNA information at the outset or during the course of an investigation should be clearly defined.

we further recommend an amendment, in the case of investigations involving child abuse/child pornography and threats to national security, to stipulate that TSPs shall cooperate with law enforcement.

Thank you for the opportunity to participate.

Respectfully submitted,

Heidi Illingworth
Executive Director

Customer Name and Address Consultations
Submitted by: Canadian Resource Centre for Victims of Crime

□

CUSTOMER NAME AND ADDRESS

CONSULTATIONS

Public Safety Canada

By: Canadian Resource Centre for Victims of Crime
October 10, 2007

□
Introduction

The Canadian Resource Centre for Victims of Crime (CRCVC) is a non-government, non-profit advocacy group for victims and survivors of violent crime. We provide direct assistance to victims across the country as well as advocate for more services and protections for victims and the public. We were pleased to receive an invitation from Public Safety Canada to participate in the consultation process regarding possible measures to address law enforcement and national security agencies' lawful access to customer name and address (CNA) information held by telecommunications service providers (TSPs).

As a non-government organization dedicated to ensuring the voice of victims and survivors is heard, we agree that the rights and freedoms guaranteed in the Canadian Charter of Rights and Freedoms must be protected. However, the protection of an individual's privacy cannot take precedence over the protection of the public from national security threats or the protection of children from sexual exploitation.

Canada is in no way immune to terrorist threats, as seen with the arrest of a Quebec man in connection with an online plot to bomb targets outside Canada on September 14, 2007. If not for the prompt response of the RCMP and other law enforcement groups, a serious incident may have occurred.

We have long advocated for increased protections for child victims; including those who may be sold, prostituted or used for child pornography. Our largest area of focus has been on advocating for increased resources for law enforcement to allow them to fully investigate and rescue children from sexual exploitation on the Internet.

As stated in the consultation document, law enforcement has repeatedly voiced their concerns about the difficulty in consistently obtaining basic CNA information in the course of their duties.

Officials need prompt cooperation from TSPs in order to prevent threats to national security/public safety and to rescue abused children. It is our opinion that corporations should be

obligated to assist law enforcement (without a warrant), as any good citizen would, in preventing and investigating crime.

Customer Name and Address Consultations
Submitted by: Canadian Resource Centre for Victims of Crime

□
Our position

In 2000, the CRCVC sent a discussion paper to all Members of Parliament and Senators entitled "Child Sexual Exploitation and the Internet." We made 20 recommendations, including that legal requirements be imposed on Internet Service Providers (ISPs) to cooperate with law enforcement, the creation of a new offence of luring, raising the age of consent, creation of a national tip-line, etc. It is unfortunate that seven years later, law enforcement agencies still face challenges accessing basic CNA information.

The lack of explicit legislation in this area gives telecommunications companies the discretion to provide information to law enforcement when it is requested or to demand a court order before releasing any information at all, regardless of the situation at hand. This is problematic at any stage of an investigation, likely halting it or creating significant delays while documents to compel the information are sought. We should not have to reiterate the risk of delays in the context of preventing terrorism or rescuing children from sexual abuse. We believe the government should immediately amend section 7(3) of the Personal Information Protection and Electronic Documents Act (PIPEDA) to make it clear that 'lawful authority' does not require a warrant in order to ensure the police and national security agencies are granted CNA information.

We fully support the use of safeguards, as listed in the consultation document. In order to prevent abuses, for example, we support limits on who can have access to the information, limiting how it is used, and internal audits on the use of the powers, etc. We agree that lawful access to CNA information should not include the content of communications or the web sites an individual visited online unless a court order is issued.

Concerns of privacy advocates

The problem of child pornography on the Internet is getting worse, and despite the many successes of Canadian law enforcement, police are only able to scratch the surface. We applaud the continued, difficult work of police officers in sorting through tens of thousands of images of child pornography in order to catch the predators and stop the abuse of children. Their objectives are simple - arrest those who create, distribute and access child pornography and identify and

rescue those children who have already been harmed.

Some privacy advocates suggest, "Canadian law enforcement and national security agencies are looking for a quick and easy way to obtain access to the names, phone numbers, IP addresses, etc

Customer Name and Address Consultations
Submitted by: Canadian Resource Centre for Victims of Crime

□ of customers of Canadian telecommunications service providers. Quick and easy, in this context, means without the delay and paperwork involved in applying to a judge for a search warrant."¹ We urge officials to remember that police/national security officials seek this information in a number of contexts, including in the very beginning of investigations or as part of intelligence gathering. We submit that persons who come to the attention of law enforcement or national security agencies in the course of their investigative duties are 'persons of interest'. Their actions online have raised serious red flags. We do not believe that CNA information is sought when there is insufficient evidence to connect an individual to a crime so that a judge would not issue a warrant.

Law enforcement and national security agencies must act quickly when such 'persons of interest' come to their attention. There is not always ample time to obtain lawful authority in the form of a warrant. Immediate threats to national security and the sexual abuse of children must override the protection of anyone's personal information by PIPEDA.

We urge Public Safety officials to remember the privacy violations of the innocent children whose images are being traded like baseball cards every day for the sexual satisfaction of pedophiles and predators. There is no greater violation of privacy than having images and videos of someone raping you distributed around the world. We cannot allow these crimes to continue to be facilitated by private companies in Canada who provide broadband Internet access, virtual storage areas for abuse images and anonymous e-mail, and forums for pedophiles to support each other in the belief that having sex with children is not wrong.

Tom Copeland, head of the Canadian Association of Internet Providers, has stated that requiring a search warrant for police to get a suspect's name and address is "over-kill" and that information is not normally considered private. We agree, and would submit, that much of the "personal information" held by TSPs is already public information contained in most telephone directories.

We also submit that cooperation by TSPs on a case-by-case basis, which is what generally occurs now, is simply not good enough when it comes to the safety/protection of children

or threats to national security. Privacy advocates maintain that there must be court oversight in order to hand over personal information and that police investigations have not been hampered to date.

1 David T.S. Fraser, "Some necessary background information to the fuss over warrant-less access to Canadian personal information,"

15 September 2007.

<http://www.privacylawyer.ca/blog/2007/09/some-necessary-background-to-fuss-over.htm>

Customer Name and Address Consultations
Submitted by: Canadian Resource Centre for Victims of Crime

□ However, investigations have been hampered, as reported by many police officers during the Statutory Review of PIPEDA in 2006/2007. In our opinion, police do not and should not need a warrant to secure subscriber information or in any other circumstance except when dictated by Parliament.

Police do not need a warrant to check a license plate in order to identify the owner of a vehicle that is suspected of being involved in a crime. There are many examples where law enforcement has access to information that the average citizen does not. They have access to this information because they are tasked with preventing and investigating crime and they have an already well established legal obligation not to disclose the information that they obtain except within the course of their mandated duties.

The Problem

As PIPEDA currently exists, it requires the consent of the individual for all collection, use and disclosure of personal information, subject to a number of exceptions. "Personal information" includes any information about an identifiable individual. It is thus illegal for TSPs to disclose such information without consent.

What constitutes lawful authority is at question. Subsection 7(3)(c) of the legislation is where the confusion occurs, as it sets out provisions where an organization may disclose personal information without consent. The first condition is when it is in compliance with a subpoena, warrant or court order. The second stipulation for disclosure is in response to a request by a government institution that has the lawful authority to obtain the personal information for the purpose of enforcing a law, carrying out an investigation related to the enforcement of the law, or gathering intelligence for purposes of enforcing a law.²

It is the term lawful authority that is problematic. On December 18, 2006, the Privacy Commissioner wrote the CRCVC and stated that under section 7(3)(c.1)(ii), "the

decision to disclose the information rests with the organization...In other words, the disclosure is discretionary on the part of the organization." we submit, once again, that discretionary

2 Section 7(3)(c.1) states that an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is "made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs, (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or (iii) the disclosure is requested for the purpose of administering any law of Canada or a province;"

Customer Name and Address Consultations
Submitted by: Canadian Resource Centre for Victims of Crime

□ disclosure is simply unacceptable when it comes to public safety and the sexual exploitation of children.

CRCVC Recommendations

Given the confusion that exists regarding lawful authority and the hesitation of some TSPs to comply with law enforcement requests, we recommend (at the minimum) that section 7(3) be amended to make it clear 'lawful authority' does not mean a warrant is required. Lawful access to CNA information at the outset or during the course of an investigation should be clearly defined.

we further recommend an amendment, in the case of investigations involving child abuse/child pornography and threats to national security, to stipulate that TSPs shall cooperate with law enforcement.

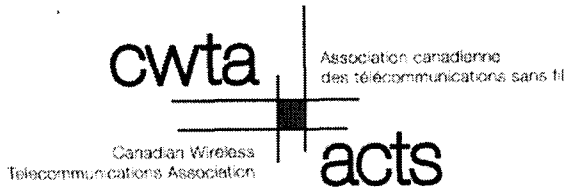
Thank you for the opportunity to participate.

Respectfully submitted,

Heidi Illingworth
Executive Director

Customer Name and Address Consultations
Submitted by: Canadian Resource Centre for Victims of Crime

□



October 12, 2007

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

RE: Customer Name and Address Information Consultation

The Canadian Wireless Telecommunications Association ("CWTA") is pleased to provide the following comments to Public Safety Canada in response to the discussion paper on Customer Name and Address information ("CNA"). CWTA is the authority on wireless issues, developments and trends in Canada. It represents cellular, PCS, messaging, mobile radio, fixed wireless and mobile satellite carriers as well as companies that develop and produce products and services for the industry.

CWTA has been actively involved in the consultative discussions about lawful access and related issues since 2002 when Justice Canada issued its first consultation paper regarding this matter. Any new lawful access requirements will ultimately affect the Association's carrier and technology members.

CWTA has consistently advocated for standards-based technical requirements, appropriate compensation for Telecommunications Service Provider ("TSP") costs, and a phased-in approach for the implementation of any newly required technical capabilities. It is the consensus view of our members that the previous legislative proposal, Bill C-74: *Modernization of Investigative Techniques Act*, failed to address those needs.

CWTA strongly urges the government to include concrete measures to address the industry's concerns in any new lawful access legislation. From a practical perspective, unless our legitimate concerns are addressed, it will be difficult for the industry to support this important initiative going forward. Any new requirements must be compatible with the standards-based technology that is available to TSPs.

Canada's telecommunications industry has a long history of working cooperatively with law enforcement within Canada's legal framework for lawful access to communications and access to customer information. While cellular/PCS licencees are the only TSPs that have any legal obligation to provide specific lawful access capabilities within their networks, all carriers have some capability and all carriers respond to law enforcement needs on a routine basis. Canadian TSPs generally, and wireless carriers in particular, maintain dedicated security departments whose sole purpose is to respond to law enforcement requests and comply with court orders. These services are provided at considerable cost to the carriers.

Personal information associated with wireless subscribers is subject to the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") rules under the Privacy Commissioner of Canada as well as the *Confidentiality of Customer Information* rules of the CRTC. PIPEDA allows the release of a subscribers' personal information when legally compelled to do so. Unlike wireline telephone numbers, the CRTC considers that wireless telephone numbers are confidential and it requires carriers to treat them as such. CRTC rules allow the release of subscriber's wireless numbers only when carriers are legally compelled to do so.

In order to comply with their obligations under PIPEDA and CRTC rules to protect their customers' privacy, wireless carriers generally require a warrant or court order before providing law enforcement agencies ("LEAs") with confidential customer information. In cases where exigent circumstances or urgent need can be demonstrated, carriers respond to LEAs as quickly and as diligently as possible.

The wireless industry would prefer to continue to provide confidential customer information only subject to court order or warrant except in exigent circumstances. CWTA does, however, agree with Public Safety Canada's observation that there is a lack of clarity for TSPs with respect to the provision of CNA. CWTA would therefore welcome clarification of the scope of CNA and the circumstances and conditions under which TSPs will be compelled to provide CNA to law enforcement. These details should be explicitly identified and clarified in whatever legislation or regulations are enacted.

As mentioned above, wireless carriers maintain dedicated security departments and incur significant costs in order to cooperate and work with LEAs. It is therefore imperative that LEAs compensate TSPs for law enforcement services. This will become even more important if the volume of CNA requests increases under the proposed "no warrant" regime suggested by this consultation. Costs for TSPs to comply will increase substantially along with the increase in requests.

With respect to the specific CNA information under consideration, much of the information listed in the consultation is already available either publicly or via CRTC tariffed services. A variety of third parties provide "reverse look-up" services for Canadian telephone numbers and many of these are provided free of charge on the public Internet. TELUS' LEADS system provides the registered customer's name and the service address of published telephone numbers. Bell's LSPID service provides LEAs with the name of the TSP associated with a 10 digit telephone number. CWTA is not aware of even a single circumstance when law enforcement has demonstrated an inability to obtain CNA information from the wireless industry.

CWTA notes that the types of "basic identifiers" sought for wireless services go well beyond what virtually anyone would consider basic and are much more onerous than those for TSPs using other technologies. IP addresses and dynamic IP addresses, IMSIs, ESNs, IMEIs, and SIM numbers go well beyond basic "tombstone data" normally associated with CNA. For the sake of fairness, consistency, competitive equity, and technological neutrality, wireless carriers should not be compelled to provide greater levels of information than other TSPs.

If the government does take action to define TSP obligations with respect to CNA, it should clearly recognize the limits of TSPs' ability to respond in a timely manner. Given that certain wireless CNA information has always been considered confidential, systems that can provide quick response for directory assistance have never been developed for wireless services. Wireless carriers work diligently to respond to LEA requests, but face constraints on their ability to provide information. These limitations may be a result of the volume of requests, the details required, or other factors, but it should be recognized in whatever requirements may be imposed that TSPs cannot always respond as quickly as may be desired.

CWTA further notes that wireless carriers do not always have any business reason to collect customer information, and so do not have verified CNA data in their possession in all circumstances. As you will

recall, CWTA addressed this in its comments to the Department of Justice Canada dated December 16, 2002:

The CWTA strongly opposes the imposition of [a provision of subscriber or service provider information] obligation beyond those situations where a wireless carrier is already collecting this information. Moreover, the CWTA is of the view that service providers should not be liable for the accuracy of customer name and/or address information. In this regard, the CWTA would note that the European Convention refers to subscriber information in that service provider's possession or control.

Generally, wireless carriers collect, validate and maintain customer information to the extent that such information is necessary to successfully provide service and to collect payment. For postpaid services (services for which the customer receives a monthly bill), wireless carriers would typically undertake a credit check to determine a prospective customer's ability to make monthly payments for the services provided. However, this process is geared to validating credit worthiness, not customer name and address. *Wireless carriers do not undertake exhaustive validation of the information that is provided by customers and wireless carriers do not warrant that such information is valid or correct, or that it would satisfy the requirements of law enforcement and security agencies.* Further, wireless carriers are almost entirely reliant on customer initiated notification with respect to address changes.

Consequently, the CWTA opposes the imposition of any obligation for service providers to collect information that they are not already collecting for their own purposes. Significant service, business and cost issues would arise if *wireless carriers were required to collect, validate and maintain accurate customer information for the purposes of lawful access.*

First, any such requirement would likely obligate wireless carriers to insist that customers present a minimum degree of official identification at the point of purchase. This would also require that wireless carriers, and the literally thousands of independent distribution agents and outlets they rely on, would be capable of validating such identification. CWTA notes in this regard the concerns raised by the Privacy Commissioner of Canada.

Second, an overwhelming issue arises with respect to on-line purchases of a wireless service since, for these purchases, the entire transaction is conducted over the Internet, not in person. Similarly, customers who opt for on-line billing will be billed on-line and will not have a monthly invoice sent to a physical address. If they chose to move, the carrier will have no means of knowing, apart from the customer taking the initiative to update this information by accessing their on-line account. In the case of purchasing or billing, on-line transactions do not lend themselves to the presentation and validation of the customer's identification. *Wireless carriers, and countless other businesses in Canada and abroad, have already made significant investments in on-line purchasing, billing and customer relations capabilities and they rely on this channel as a useful and cost-effective means by which to acquire, bill and interface with their customers.*

Third, another problem is created with respect to prepaid wireless services provided by wireless carriers since valid customer information is not required by carriers in order to provide prepaid services. Given that a credit check is not required, and that the customer will never receive a monthly bill, there is no need for the carrier to request the customer's name or address. The entire transaction of activating the customer's account can be conducted over the phone and absent any identification. Although wireless carriers are increasingly requesting customer name and address information for business purposes, this information

is not validated, nor do carriers deny service if the customer does not provide the information.

It should be noted that this situation is not isolated to wireless phones. The verification of a customer's address is only necessary when a service provider must establish a physical connection to the customer. For example; Direct Broadcast Satellite, Multipoint Distribution Service, dial-up Internet Service Providers, and prepaid local and long distance phone card providers are also capable of providing service without knowing the address of the customer.

All of the foregoing remains true today, and CWTA continues to oppose any obligation that would require TSPs to collect customer information beyond what is already collected for business purposes.

Conclusion

The CWTA recognizes that lawful access to communications and the ability to obtain CNA information are important tools for law enforcement. To function properly, however Canada's lawful access regime must recognize the realities of the telecommunications industry:

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

CWTA appreciates the opportunity to provide these comments. Given that there are no proposals in this consultation, CWTA requests the opportunity to comment on any changes the government intends to make to the current lawful access regime.

CWTA believes that the importance of this matter warrants full disclosure of the issues involved and encourages the Department to make all comments received through this consultation public. CWTA will be posting these comments on the Association's website.

Sincerely,

Filed electronically

J. David Farnes
Vice President,
Industry and Regulatory Affairs

October 12, 2007

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

e-mail: cna-consultations@ps-sp.gc.ca

The Canadian Chamber of Commerce appreciates the opportunity to provide the following comments in response to the Customer Name and Address Consultation. The Canadian Chamber is Canada's largest and most representative business association. We speak for 170,000 businesses of all sizes and sectors through our 350 local chambers of commerce and boards of trade located in every province and territory.

The Canadian Chamber's telecommunications service provider (TSP) members have a long history of cooperation with Canada's law-enforcement and national-security agencies (LEAs) and of facilitating lawful access to electronic communications - subject to appropriate legal process and judicial oversight. That being said, the Canadian Chamber agrees that there is a lack of clarity for TSPs with respect to the provision of customer name and address (CNA) information. The Canadian Chamber would welcome clarification of the scope of CNA and the circumstances and conditions under which TSPs will be compelled to provide this information to LEAs.

TSP subscribers' personal information is subject to the Personal Information Protection and Electronic Documents Act (PIPEDA), as well as the Canadian Radio-television and Telecommunications Commission's (CRTC) Confidentiality of Customer Information rules. PIPEDA allows the release of subscribers' personal information without consent only in limited, explicitly itemized circumstances. One such exemption allows disclosure without subscriber consent when an organization is legally compelled to do so under a court order, warrant or where otherwise required by law. Consistent with PIPEDA and CRTC rules, TSPs generally require a warrant or court order before providing LEAs with customer information.

In taking steps to clarify TSPs obligations to provide CNA information to LEAs, there are limits to a TSP's ability to provide certain CNA information as quickly as may be desired by LEAs. TSPs face constraints upon their ability to provide information which can

Canadian Chamber of Commerce.txt

come as the result of the volume of requests and the CNA information available to them.

The Canadian Chamber notes that Canadian TSPs desire to continue their positive relationships with LEAs. In addition, mandated data retention requirement could impose significant and unwarranted storage and processing costs on Canadian TSPs and their law-abiding customers.

The Canadian Chamber has consistently advocated for the following if lawful access legislation was introduced:

□

- internationally-recognized standards for lawful access technical requirements;
- a reasonable transition period (i.e. 12 months) from the time any new lawful access legislation comes into force to when TSPs must implement compliant solutions;
- compensation for the costs incurred in:
 - o executing warrants/court orders
 - o implementing non-standard lawful access capability requirements
 - o implementing lawful access capability requirements on an urgent basis, prior to a reasonable transition period (i.e. 12 months)

Once again, the Canadian Chamber of Commerce appreciates the opportunity to provide comments on this very important issue.

Sincerely,

Michael Murphy
Executive Vice-President, Policy

□

CIPPIC.txt

Université d'Ottawa .. University of Ottawa
Faculté de droit .. Faculty of Law
57 Louis-Pasteur, Ottawa (Ontario) K1N 6N5 Canada
(613) 562-5800 (2553) .. (613) 562-5417 (Télec/Fax)
www.cippic.ca .. cippic@uottawa.ca
Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada
Philippa Lawson
Director
(613) 562-5800 x2556
plawson@uottawa.ca
October 15, 2007

BY EMAIL AND MAIL
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON
K1A 0P8

Dear Sir/Madam:
Re: Customer Name and Address Consultation

1. The Canadian Internet Policy and Public Interest Clinic ("CIPPIC") is a legal clinic based at the University of Ottawa, Faculty of Law. CIPPIC's mandate includes intervening in legal and policy-making processes on issues arising from the use of new technologies, the outcomes of which have broad public interest implications. Our goal is to ensure that important public interest voices are heard in the policy-making process so that results reflect more than strong vested interests.

2. Public Safety Canada, in collaboration with Industry Canada, has initiated a public consultation on the issue of "updating Canada's lawful access provisions as they relate to law enforcement and national security officials' need to gain access to CNA [Customer Name and Address] information in the course of their duties."¹

3. The following are CIPPIC's comments in response to the Consultation Paper.
Background

4. The government's Consultation Paper sets out law reform proposals that closely reflect those proposed by the Liberal government two years ago in Bill C-74, the Modernization of Investigative Techniques Act, which died with the 38th Parliament when an election was called shortly thereafter. An identical bill was later introduced by Liberal M.P. Marlene Jennings as a private member's bill (Bill C-416), but this bill also died on the order paper when Parliament was prorogued.

¹ See "Customer Name and Address Information Consultation" Document, Online: <<http://securitepublique.gc.ca/prg/ns/cna-en.asp>>. □

2

5. The proposals to give law enforcement agencies easier access to basic information about telecommunications subscribers have been mooted by the federal government for a number of years. In 2002, the Canadian government announced plans to modernize its

criminal law
and establish new rules regarding "lawful access" in light of the challenges posed
by new
technologies to law enforcement. That year, the government consulted with
stakeholder
groups, including civil society, on a number of ideas including the creation of a
national
CNA database. Over 300 submissions were received, many from individuals and
organizations concerned about the potential impact of the proposals on privacy and
civil
liberties.

6. In early 2005, government officials initiated targeted, closed consultations
with stakeholders
(including industry and civil society) on revised proposals, having taken into
account the
input received in earlier consultations. The revised proposals included
"warrantless" access
to CNA information.²

7. In both sets of consultations, civil society raised serious concerns about the
impacts of the
proposals on the privacy and civil liberties of individuals, and expressed
opposition to
proposals for warrantless access to subscriber data. CIPPIC has summarized the
consultations and views expressed by civil society in a webpage located at
<http://www.cippic.ca/projects-cases-lawful-access/>. This webpage also includes
links to
written submissions and other relevant documents.

8. Bill C-74, the Modernization of Investigative Techniques Act, was introduced in
November
2005. Among other things, the bill included provisions requiring telecommunications
service
providers to hand over certain subscriber identifying information to law
enforcement
agencies upon request, without any need for reasonable grounds to suspect criminal
activity
and without a court order, warrant, or other judicial authorization. The bill did
not get past
First Reading before an election was called.

9. The current Consultation focuses on essentially the same proposal for
warrantless access by
law enforcement agencies to customer name and address ("CNA") information from
telecommunications service providers.

10. According to the most recent consultation paper, "[t]he objectives of this
process are to
maintain lawful access for law enforcement and national security agencies in the
face of new
technologies while preserving and protecting the privacy and other rights and
freedoms of all
people in Canada," while ensuring "that the solutions adopted do not place an
unreasonable
burden on the Canadian public."

The Problem

11. The proposals in question are designed to address problems currently being
experienced by
law enforcement agencies. The Consultation Paper explains the problem as follows:
2 By "warrantless access", we mean the right to demand and obtain such information
without a warrant, court order,

or other judicial authorization, and without reasonable grounds to suspect criminal activity. □

3

Law enforcement agencies have been experiencing difficulties in consistently obtaining basic CNA information from telecommunications service providers (TSPs). In the absence of explicit legislation, a variety of practices exists among TSPs with respect to the release of basic customer information, e.g., name, address, telephone number, or their Internet equivalents. Some companies provide this information voluntarily, while others require a warrant before providing any information, regardless of its nature or the nature of the situation. If the custodian of the information is not cooperative when a request for such information is made, law enforcement agencies may have no means to compel the production of information pertaining to the customer. This poses a problem in some contexts. For example, law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation. The availability of such building-block information is often the difference between the start and finish of an investigation.

12. The problem thus seems to have two distinct aspects:

- a) locating next of kin in emergency situations, and
 - b) gathering CNA information during the early stages of an investigation.
- Locating next-of-kin in emergency situations

13. With respect to the former, the appropriate solution is to require that TSPs hand over the necessary information upon request for the purpose of locating next-of-kin in an emergency situation; it is not to allow police to demand such information for the much broader purpose of "performing an official duty or function". Especially where fundamental civil liberties are at stake (see below), solutions should be tailored to the problem at hand. Gathering CNA information in early stages of investigations

14. The second aspect of the problem, as stated in the Consultation Paper, is more troubling. It is not clear whether the problem here involves situations where:

- a) the police have reasonable grounds to suspect criminal activity but need to act immediately and don't have time to obtain a warrant;
- b) the police have reasonable grounds to suspect criminal activity but simply don't want to go through the process of obtaining a warrant; or
- c) the police lack reasonable grounds to suspect criminal activity and therefore can't get a warrant to obtain the information.

15. In the first situation, section 487.11 of the Criminal Code allows police to engage in searches without a warrant "if the conditions for obtaining a warrant exist but by reason of exigent circumstances it would be impracticable to obtain a warrant." Presumably, the problem here is that the police can't obtain the information in question without the cooperation of the TSP, and some TSPs are not cooperating. As with the emergency situation described above, this situation can and should be addressed with provisions tailored to the problem in question.

Thus, if the problem is that TSPs are refusing to hand over subscriber information regarding someone the police have reasonable grounds to believe is engaging in criminal activity, and if the urgency of the matter justifies proceeding without a warrant, then the proposed law should permit the police to demand production of information where such criteria are met. □

4

In practical terms, the police officer requesting the information from the TSP should be required to communicate the grounds for the request to the TSP, as well as to record it for audit purposes.

16. If police simply want to be relieved of the administrative effort of obtaining warrants for CNA information in cases where they have reasonable grounds, we again submit that the proposed solution is too broad. First, it is not clear how the public will benefit by relieving the police of due process requirements in cases that do not involve exigent circumstances. More evidence of how due process requirements regarding CNA information are currently impeding legitimate investigations is needed before mandating disclosure without a warrant requirement. Second, as noted below, CNA information, especially in the digital context, is much more than mere "tombstone" data. It can open the door to a host of detailed information about the individual. We therefore see no reason to apply a lower threshold for access to CNA information than to other information about subscribers.

17. Assuming, however, that there is good reason to relieve police of the warrant requirement for CNA information (as opposed to other information) where they have reasonable grounds to suspect criminal activity, then once again, the proposed solution is too broad. Binding requests for CNA information should be limited to those made for the purpose of investigating suspected criminal activity where the requestor has reasonable grounds to believe that a crime is being, has been, or will be committed. Even if third party authorization is not required, "reasonable grounds" can be required and police can be held accountable after the fact. As noted above, the police officer making the request should be required to state the grounds for the request to the TSP, and to record it along with relevant evidence for audit purposes.

18. If, on the other hand, the problem is that the police want to be able to gather CNA information when they have no reasonable grounds to suspect criminal activity, we submit that the proposal is unacceptable. Such requests, in our view, constitute "fishing expeditions" and violate fundamental principles of due process. In free and democratic societies, police should not be engaging in proactive investigations without any reasonable grounds to suspect criminal activity. To allow such investigations is to invite abuse. We

doubt that it would withstand a Charter challenge. Our laws of due process have been carefully crafted so as to balance police powers with civil liberties. Allowing what amount to forced searches without any requirement for reasonable grounds to suspect criminal activity would upset this balance.
Definition of "lawful authority" in subs.7(3)(c.1), PIPEDA

19. Although not stated in the Consultation Paper, we understand that there is another problem underlying the proposal for easier access to CNA information. According to law enforcement agencies and victim rights advocates, some TSPs demand warrants before handing over CNA information because they interpret subs.7(3)(c.1) of the Personal Information Protection and Electronic Documents Act ("PIPEDA") as requiring such ⁵ authorization.³ PIPEDA contains a number of exceptions to the general rule that organizations must not disclose information about identifiable individuals (including CNA information) without consent. These exceptions include the following:
(c) [where] required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;
(c.1) [where] made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that
(i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
(ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or
(iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

20. The term "lawful authority" in subs.7(3)(c.1) is not defined in the Act. Apparently, it is being interpreted by some TSPs as requiring authorization in the form of a warrant, court order, or other judicial authorization.⁴ Hence, some TSPs consider themselves prohibited from disclosing CNA (and other personal) information to the police unless the request is accompanied by a warrant.

21. It is our understanding that this interpretation was not intended by the drafters of PIPEDA or by Parliament when it passed PIPEDA. Subs.7(3)(c) already provides for disclosures in response to warrants, court orders, etc. Subs.7(3)(c.1) was added in order to preserve the status quo, under which organizations were free to disclose personal information to law enforcement agencies even without any warrant or other formal authorization. The term "lawful authority" was meant, we believe, to refer to the institution's authority,

not to due process requirements. Although we support those organizations that choose not to disclose other than in response to warrants, it is our understanding that PIPEDA gives the organization discretion to make that choice; it does not prohibit such disclosures.

22. To the extent that the problem underlying these proposals stems from this misinterpretation of subs.7(3)(c.1) of PIPEDA, we submit that the appropriate response is to define "lawful authority" in PIPEDA. It is not to substantially change the law so as to remove the discretion of organizations to demand warrants before handing over their subscribers' identifying information.

3 See Submissions and Testimony of the Canadian Chiefs of Police and the Canadian Resource Centre for Victims of Crime to the House of Commons Standing Committee on Access to Information, Privacy and Ethics in its review of PIPEDA, Meeting No.30, Feb.13, 2007, online: <<http://cmte.parl.gc.ca/Content/HOC/committee/391/ethi/evidence/ev2695445/ethiev30-e.htm#Int-1895029>>

4 Hereinafter, we use the term "warrant" to cover all forms of court orders or judicial authorization. □

6

Reasonable expectations of privacy in CNA Information
23. According to the consultation paper, the proposals are designed to assist law enforcement and national security agencies in determining the identity of telecommunications service subscribers, and "would not, in any formulation, include the content of communications or the web sites and individual visited while online." The CNA information in question "could include the following basic identifiers associated with a particular subscriber":

- name;
- address(es);
- ten-digit telephone numbers (wireline and wireless);
- Cell phone identifiers, e.g., one or more of several unique identifiers associated

with a subscriber to a particular telecommunications service (mobile identification

number or MIN; electronic serial number or ESN; international mobile equipment or IMEI number; international mobile subscriber identity or IMSI number; subscriber identity module card number of SIM Card Number);

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

24. If this proposal were to go forward, it is essential that the scope of information subject to the new rules be highly constrained (certainly, no broader than in this proposal) and not subject to expansion in future years. This is best done by including the definition in legislation, not ancillary regulations.

25. However, the proposal for warrantless access to CNA information is questionable insofar as it is based on the premise that CNA information attracts a lower expectation of

privacy than does other (e.g., message header or content) information associated with individuals. While names and addresses may generally attract a lower expectation of privacy than do other types of personal information, that is not necessarily true - especially in the electronic context. Names and addresses can be keys to a host of sensitive personal information such as financial records and health details, much of it available by simple internet searches. As some commentators have noted, allowing unfettered access to CNA information: ...will bestow upon law enforcement officials a reservoir of personal information from which to fish. These deep basins will allow officials to cast their nets wide, enabling access to personal information that reveals core biographical data... typical subscriber information of the sort made available under the proposed ... scheme will become the means by which a biographical core of personal information is assembled .5
5 Daphne Gilbert, Ian R. Kerr and Jena McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers," (2007) Criminal Law Quarterly, vol. 51(4) 469 at 502-503 [citing, in part: Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age (New York: New York University Press, 2004)].

□
7

26. Many people use pseudonyms on the Internet in order to engage in anonymous communications without fear of embarrassment or retribution. They have a high expectation of privacy in relation to their Internet identities, and reasonably so. Unmasking their identities without any kind of judicial authorization or requirement for reasonable cause to suspect criminal behaviour is not consistent with the values of a free and democratic society, and may indeed violate the Canadian Charter of Rights and Freedoms.⁶
Charter implications

27. Section 8 of the Canadian Charter of Rights and Freedoms provides everyone with "the right to be secure against unreasonable search and seizure."⁷ According to the Supreme Court of Canada, s.8 protects people, not places or property.⁸ The Court has also found that the protection in s.8 is based on "reasonable expectations of privacy"⁹, and that everyone has a reasonable expectation of privacy in their "biographical core of information"- i.e., information which tends to reveal intimate details of the lifestyle and personal choices of the individual.¹⁰ Because CNA information (e.g., IP addresses and associated subscriber names) can easily be linked with online activities and communications that expose intimate details of an individual's life, it engages reasonable expectations of privacy, and thus section 8 of the Charter.

28. In order for a search to be considered "reasonable" under section 8, courts have found that there must be "reasonable and probable grounds" to suspect that a crime has been

committed.¹¹ Practically speaking, and most often, this means that a search and seizure must be judicially authorized, after the judge has been satisfied that there are reasonable and probable grounds to believe criminal activity has taken place or will take place.¹²

29. Exceptions to this fundamental rule of due process may be permitted under section 1 of the Charter if they "can be demonstrably justified in a free and democratic society." The Supreme Court has set out the following test to determine whether a given measure can be so justified:

- There must be a pressing and substantial objective; and
- The means must be proportional; which implies that:
 - (i) the means must be rationally connected to the objective;
 - (ii) there must be minimal impairment of rights; and
 - (iii) there must be proportionality between the infringement and objective.¹³

30. We question whether the proposal for warrantless access to CNA information would pass

Charter scrutiny, given the less invasive law reforms that could be implemented to address

6 Ibid.

7 Section 1 of the Charter, however, allows for "such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."

8 Hunter v. Southam Inc., [1984] 2 S.C.R. 145, at para 23, Dickson citing Katz v. United States, 389 U.S. 347 (1967).

9 Ibid. at para 24.

10 R. v. Plant [1993] 3 S.C.R. 281 at 293.

11 Supra note 2 at para 43.

12 Supra note 2 at para 28-29.

13 R. v. Oakes, [1986] 1 S.C.R. 103, 24 C.C.C. (3d) 321, 50 C.R. (3d) 1 at paras 69-71. □

8. the problems raised by law enforcement agencies (see above), and the disproportionate impact on individual privacy that warrantless access to CNA information would have,

especially in light of the weak oversight and accountability mechanisms currently in place for law enforcement agencies in Canada.

31. Moreover, the internet is a vibrant forum for expression of political dissent and unpopular views, as well as for the sharing of highly personal information, in large part because of the anonymity that it offers to people. In this context, individuals should not be stripped of their anonymity without due process. Otherwise, valuable free speech (as protected by section 2 of the Charter) will be chilled.

32. CIPPIC submits that Canadians have a reasonable expectation of privacy in their CNA information, that forced access to that information constitutes a search and seizure, and that such a search therefore requires prior authorization based on reasonable grounds to suspect criminal activity. Allowing for such searches without warrants or other judicial authorization on a "reasonable grounds" basis would, in our submission, violate the Charter.

Safeguards

33. The primary safeguard against police abuse of investigative powers is the requirement for prior judicial authorization before a search or other surveillance activity takes place, based on a "reasonable grounds" standard. The proposal in question would do away with precisely that safeguard. For this reason, we object to it.

34. Another critical safeguard is the existence of effective oversight mechanisms to guard against and punish abuse of power. As the Arar Commission's report makes clear, current oversight mechanisms for Canadian national security and law enforcement agencies have proven themselves inadequate in preventing inappropriate sharing of personal information among law enforcement agencies.¹⁴ Without improvements to our current oversight mechanisms, we should not be granting any additional powers to law enforcement agencies.

35. In this respect, we support the Ontario Information and Privacy Commissioner's call for the creation of an independent oversight body to supervise lawful access activities of law enforcement agencies and ensure public accountability, transparency, and scrutiny, and to enhance public confidence, especially if any new "lawful access" powers are granted to law enforcement agencies.¹⁵

36. The Consultation Paper proposes a number of "possible safeguards", some of which are aimed at oversight. These include:
¹⁴ Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Report of the Events Relating to Maher Arar: Analysis and Recommendations (Ottawa: Public Safety and Emergency Preparedness Canada, 2006). Online: <http://www.ararcommission.ca/eng/AR_English.pdf>
¹⁵ The Ontario Information and Privacy Commissioner proposed such a body in its submission to the Minister of Justice and Attorney General of Canada on the 2005 "Lawful Access" Consultations. See <<http://www.ipc.on.ca/index.asp?layid=86&fid1=105>> □

- 9
- requiring regular internal audits by agency heads to ensure that any requests for CNA information are being made in accordance with the protocols and safeguards in place;
 - reporting to responsible ministers on the result of any internal audits;
 - provision of any audit results to the Privacy Commissioner of Canada, the Security Intelligence Review Committee, or provincial privacy commissioners, as appropriate; or
 - provision for the Privacy Commissioner and SIRC to conduct audits related to the release of CNA information.

37. In our submission, internal auditing requirements and discretionary external audits by the Privacy Commissioner of Canada and SIRC are insufficient. Agencies have a strong disincentive to revealing their own errors and weaknesses. Moreover, existing oversight

bodies often lack the resources to take on new tasks that they are not mandated to take on.

For these reasons, effective oversight should include:

- a mandatory external audit;
- mandatory reporting to the Minister and oversight agencies; and
- a mechanism for public accountability (e.g., reporting to Parliament; publishing of reports).

38. The Consultation Paper suggests a number of other possible safeguards, including:

- clear limitations on what customer information could be obtained upon request;
- limiting the number of employees who would have access to CNA;
- requiring that individuals with access be designated by senior officials within their organizations; limiting requests to those made for the purpose of performing an official duty or function;
- requiring that requests be made in writing, except in exceptional circumstances;
- requiring that designated officials provide associated information with their request, e.g., identification of a specific date and time for a request relating to an IP address;
- requiring designated officials to record their status as such when making a request, as well as the duty or function for which a particular request is made;
- limiting the use of any information obtained to the agency that obtained it for the purpose for which the information was obtained, or for a use consistent with that purpose, unless permission is granted by the individual to whom it relates.

39. In order for auditing and accountability mechanisms to be effective, officers accessing CNA information should be required to keep detailed records including the purpose for demanding access - not just "the duty or function for which a particular request is made".

40. With respect to safeguards against misuse of information gathered, we submit that there should be strict limits on disclosure as well as use of the information gathered. Moreover, there should be stiff penalties for opportunistic use, or misuse of information accessed through the new power.

41. Even with all these safeguards, however, the proposal to permit warrantless access to CNA information remains in our view fundamentally flawed due to its over-broad nature - i.e., permitting access without warrant or reasonable grounds as long as it is "for the purpose of performing an official duty or function". If law enforcement agencies are to be granted wider powers of access to this information, a key safeguard is to limit the purposes for which they can demand access much more narrowly than this.

Conclusion

42. Information identifying telecommunications subscribers can be highly sensitive even though the electronic trail of publicly available and otherwise accessible data that individuals now leave about themselves on the internet and other digital devices as they go about their daily lives. For this reason, we submit that CNA information raises a "reasonable expectation of privacy"

on which a Charter challenge to laws permitting warrantless access could be based.

43. Moreover, we remain skeptical about the need for these potentially intrusive and far-reaching measures. It is not clear that greater access by law enforcement to electronic communications will, in fact, increase the security of Canadians; and it has not been demonstrated that no other, less privacy-intrusive, measure would suffice to achieve the same purpose of enhanced security. In particular, the permitted purposes for demanding NA information are far broader than required to solve specific problems such as gaining access to next-of-kin information in emergency situations, or acting on tips quickly in exigent circumstances.

44. Finally, the safeguards proposed are insufficient, in our view, to protect individuals from over-reaching and abusive exercise of police powers. In particular, there should be no expansion of police investigatory powers without a corresponding increase in independent oversight.

10

Canadian Bar Association.txt

October 18, 2007

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security Branch
Public Safety Canada
269 Laurier Avenue West
Ottawa, ON K1A 0P8

Dear Ms. Clairmont:

Re: Customer Name and Address Information Consultation

I write in response to your letter dated September 11, 2007, seeking our comments on Public Safety Canada's Customer Name and Address (CNA) Information Consultation Document. This letter summarizes the Canadian Bar Association's (CBA) concerns about proposals pertaining to law enforcement and national security agencies' access to CNA information held by telecommunications service providers (TSPs). Thank you for the opportunity to contribute our views on this important subject.

The CBA is a national professional organization representing over 37,000 lawyers, notaries, law students and teachers from every part of Canada. The CBA's mandate includes seeking improvements in the law and the administration of justice.

Fundamental Principles

In previous consultations on what have been referred to as "lawful access" proposals in 2002 and

2005, the CBA emphasized several fundamental principles. We stressed that all initiatives must be constitutionally valid and reflect fundamental values of Canada's Charter of Rights and Freedoms. As a prerequisite to any new investigative powers, we noted that the need for those new powers must be clearly demonstrated and that the measures proposed be carefully tailored to provide the maximum respect for individual rights. We have previously articulated the fundamental importance of the balancing process required as follows:

□ Living in a democracy requires that the state should not interfere with, or restrict the rights, liberty or security of individuals without a demonstrated need. Where there is compelling evidence of such a need, the law or other action of the state should be tailored so that the restriction on, or interference with individual rights is no greater than absolutely necessary to accomplish the objective of the law or state action.¹

We repeat that the twin principles of demonstrated necessity and minimal intrusion must form the foundation of any proposals to advance or extend search and seizure powers. This foundation also provides the essential context in which the constitutional validity and efficacy of new measures must be assessed.

The CBA has also previously expressed strong concerns about the potential of various lawful access proposals to profoundly impact the privacy of individual Canadians. We have particularly noted, amongst our other concerns, the potential to destroy solicitor client privilege by violating communications between lawyers and clients.²

While we appreciate that access to CNA information has been the subject of previous consultation, the rapid evolution of technology and investigative practice requires careful consideration of the context in which these current proposals are made. In our view, the present context is not described in sufficient detail to permit definitive conclusions about these proposals. However, we believe that this consultation provides an opportunity to articulate a principled framework in which these issues can properly be considered.

Explicit Legal Authority

As noted in the consultation document, a wide variety of practices have developed regarding the release of CNA information to law enforcement authorities. The CBA welcomes recognition of the need for explicit legal authority for the mandatory release of this personal

information.

The inconsistent practices of Canadian organizations in general and TSPs in particular, as mentioned in the consultation document, are a direct result of the challenges many organizations have in applying the Personal Information and Electronic Documents Act (PIPEDA), specifically section 7(3). PIPEDA provides a regime that governs the collection, use and disclosure of personal information by the private sector, generally requiring knowledge and consent of the individual to whom the personal information pertains. However, section 7(3) also provides for specific limited circumstances where personal information may be collected, used and disclosed without an individual's consent. Relevant to this consultation are section 7(3)(c) regarding warrants and court orders, section 7(3)(c.1) where a request is made by a government institution that has identified its lawful authority, and section 7(3)(i) where the disclosure is "required by law".

The circumstances when a warrant or court order is presented or when disclosure is required by law elicit little confusion. However, there has been significant uncertainty and confusion as to exactly what "lawful authority" includes in relation to requests from law enforcement agencies (LEAs). A detailed analysis of "lawful authority" as intended in section 7(3)(c.1) is beyond the

1 Canadian Bar Association, Submission on Lawful Access (Ottawa: CBA, 2005) at 1.

2 Canadian Bar Association, Letter from then CBA President B. Tabor to then Ministers of Justice, Public Safety and Industry (Ottawa: CBA, 5 July 2006).

□ parameters of this consultation. However, it is relevant to note that some LEAs point to this section of PIPEDA as actually constituting their "lawful authority" to obtain the requested information. Certain LEAs have even formulated a "letter of authority" to request CNA information, referring to PIPEDA as their lawful authority.

In fact, section 7(3)(c.1) cannot constitute lawful authority to obtain the requested information. Rather PIPEDA establishes a discretionary regime pursuant to which organizations may disclose personal information when the relevant requirements of the section in question have been met.

The effect of the amendments proposed in the consultation document would be to

remove
uncertainty for certain private sector organizations (i.e. TSPs) as to any
discretion to disclose the
CNA information specified in the consultation document: according to the proposals,
they would
be "required by law" to disclose the specified information. However, while the
consultation
document clarifies the nature of an order that would give rise to an obligation to
disclose, we
note that private sector organizations would continue to have discretionary ability
to disclose
certain information pursuant to applicable privacy legislation such as PIPEDA.

Prior Judicial Authorization and Reasonable Expectations of Privacy

The consultation document proposes an administrative scheme where a designated
officer could
demand disclosure of CNA information. Several possible safeguards are suggested in
the
consultation document, many that appear to respond to some of the issues raised in
earlier
consultations.³ We have two principal concerns regarding the model proposed in the
consultation document.

First, the disclosure of the stipulated information upon demand appears to be at
least partly based
on the idea that PIPEDA would not restrict disclosure of certain material because
it is already in
the public domain through sources such as telephone directories. In fact, PIPEDA
does not
distinguish between sensitive and non-sensitive information in this context. PIPEDA
does
permit the disclosure of personal information that is both publicly available and
specified by the
regulations. However, most of the information listed in the consultation document
is not actually
publicly available and is also not specified by the regulations. Still, as noted,
disclosures in such
contexts fall under a discretionary responsibility and the other PIPEDA provisions
would
continue to apply to any discretionary disclosure.

Second, the scope of the information listed in the consultation document is much
too broad, and
extends beyond what might be appropriately regarded as "basic information".
Responses to
previous consultations on this topic also expressed concern about the scope of
proposed lists.⁴

Concerns about the scope and nature of such information must be measured against
the
constitutional concept of a reasonable expectation of privacy. This concept defines
the threshold
at which prior judicial authorization for a search will be required.⁵ However, it
is sometimes
difficult to determine precisely where that threshold will fall. The Supreme Court
of Canada has

3 See for example the response of the Federal Privacy Commissioner to a similar proposal in 2005, "Response to the Government of Canada's "Lawful Access Consultations", available online at http://www.privcom.gc.ca/information/pub/sub_la_050505_e.asp

4 Ibid.

5 See for example, *Canada v. Southam Inc.*, [1984] 2 S.C.R. 145.

□ noted that the determination of where a reasonable expectation of privacy will be found is a contextual exercise, requiring a careful balance between the rights of the individual and the legitimate interests of society in effective law enforcement.⁶ As technology and investigative practices evolve, previously constitutional activities conducted without warrant may require a warrant. The extent to which changes in technology and practice enable the discovery of "core biographical information" or reveal "intimate details regarding lifestyle" may necessitate prior judicial authorization.⁷ Further, the current technological capability to combine various sources of information to reveal additional details about individuals is a significant factor that may favour prior judicial authorization.⁸ The CBA believes that a continuing review of any administrative model would be imperative to ensure that changes in technology and practice do not result in a process that violates the Charter.⁹

Administratively authorized search procedures, as opposed to court ordered procedures, have been particularly susceptible to abuse. In the United States, a recent review of "National Security Letters" issued pursuant to the Patriot Act revealed significant irregularities and abuse in the program.¹⁰ The Office of the Inspector General documented that the use of National Security Letters increased exponentially after that power was expanded in the Patriot Act.¹¹ Difficulties and discrepancies in internal record keeping practices and controls complicated the task of compiling accurate statistics.¹² The American experience should serve as a warning for Canada in relation to administrative programs, and illustrates that significant problems can arise even when a program includes internal restrictions and safeguards.

On a practical note, careful consideration must be given to the impact of increased internal procedures and protocols on the ultimate speed and efficiency suggested as advantages of the administrative model. One result of the appropriate proliferation of internal protocols and safeguards may be to narrow any difference in the time involved between the

administrative and judicial authorization process. If this gap is significantly narrowed, diminished practical benefits of the administrative approach must be assessed against the shortcomings and difficulties of that approach noted above. It is important to consider that internal safeguards cannot replicate certain benefits of prior judicial authorization, such as those associated with maintaining public confidence in our laws. Careful consideration must also be given to existing mechanisms contained in the Criminal Code that either enable searches for certain information at lower thresholds, or through the use of an expedited process.

6 R. v. Tessling 2004 S.C.C. 67 at paras. 17-18. See also R. v. Plant, [1993] 3 S.C.R. 281 at 293.

7 Tessling, *ibid.*, at paras. 59-62.

8 For example, the impact of new technology on the ability to combine such sources, together with the resulting loss of privacy is described in the context of "data mining" in Renee Pomerance, "Redefining Privacy in the Face of New Technologies: Data Mining and the Threat to the 'Inviolable Personality'" (2006) 9 Can. Crim. L. Rev. 273.

9 We appreciate that Public Safety Minister Stockwell Day has stressed that personal information requires the ongoing protection of judicial authorization.

10 A Review of the Federal Bureau of Investigation's Use of National Security Letters", March 2007, United States Department of Justice, Office of the Inspector General, Executive Summary at 34-50. Available online at <http://www.usdoj.gov/oig/special/s0703b/final.pdf>

11 *Ibid.*, at 17.

12 *Ibid.* at 17-19.

□
In our responses to the last two consultation documents on lawful access in 2002 and 2005 and elsewhere, the CBA suggested that a comprehensive approach to search and seizure powers in the Criminal Code is needed. Such an approach should encompass all forms of search and seizure in a dedicated part of the Code, including intercepts, CNA information, tracking warrants, general warrants and other types of search and seizure.

Finally, the consultation document suggests that information could be obtained for purposes of notification of next of kin or other similar circumstances. However, it would be a relatively uncomplicated matter to deal with such situations. For example, TSPs might notify individuals

involved that the authorities have information to provide to them, or specific legislation could be passed to directed TSPs to provide CNA information in that context without prior judicial authorization. However, that unique context is significantly different than an investigation of a Criminal Code offence.

Role of the Police, CSIS and the Competition Bureau

The CBA is particularly concerned with the suggestion that the proposed powers should be granted concurrently to the police, CSIS and the Competition Bureau. The uses to which information may be put in the context of investigations by the Competition Bureau or CSIS differ significantly from that of LEAs under the Criminal Code.

In our submissions to the Air India Inquiry,¹³ the CBA pointed out that information gathered for intelligence purposes is inherently different than information gathered for law enforcement purposes. Information for intelligence purposes is gathered without the expectation that it will ultimately be led as evidence in a court of law. The procedures for gathering, storing, recording and disclosing security information is completely different from that engaged in by police officers in respect to evidence under the Criminal Code. Generally, the actions of intelligence officers will never be subject to judicial review. Accordingly the requirement for prior judicial authorization is more, not less, pressing in the case of CSIS or any other agency involved in information gathering for intelligence purposes. As has unfortunately been seen in the Arar Inquiry,¹⁴ intelligence information can be used to have devastating effect on a person's life, without any judicial intervention or review.

Likewise the nature of the Competition Act and the investigations conducted by the Competition Bureau under that Act are quite different from the type of investigation carried on by the police. In the context of the Competition Act, it is anticipated that voluminous documentation would be an inherent part of the process and that the breaches of law will be aimed primarily at unlawful financial advantage as opposed to threat of physical harm. Realistically, the Competition Bureau is unlikely to require CNA information on an urgent basis such that the absence of prior judicial authorization would be justified.

Conclusion

The CBA appreciates the opportunity to participate in ongoing consultations regarding lawful access and access to CNA information. We have stressed that the determination of

constitutional norms in this regard is a context sensitive exercise. Any expansion of the search powers in the

13 Canadian Bar Association, Submission to the Air India Inquiry (Ottawa: CBA, 2007).

14 Canadian Bar Association, Submission to the Arar Inquiry (Ottawa: CBA, 2005).

□ Criminal Code or other legislation should not occur without a clear and demonstrable foundation. We welcome the opportunity to participate in further discussions once that context has been fully articulated, particularly in relation to present technical and practical capabilities.

We have noted several difficulties with an administrative search regime. The constitutional status of such a regime may be undermined by technological advances, changes in practice or the ability to combine or aggregate data from several sources. Further, there are inherent difficulties with an administrative approach such that it may be that in the long run a system based on prior judicial authorization provides the more constitutionally stable and effective approach. Finally, to the extent that the consultation document proposes a "one size fits all" approach for the Criminal Code, the Competition Act, and CSIS, we express our concern, and point to the very distinct roles of these statutes and agencies and the contexts in which they generally function. A proper approach must recognize those significant differences.

The issue of costs of complying with either a court order or an administrative order is a complex and contentious one. It is difficult to compare costs of an administrative scheme with one that relies on court orders, given factors such as indirect cost implications to the court system or direct cost implications to the law enforcement agency involved. The current proposals may also have cost implications for TSPs and other third parties. This has been the subject of other consultations, and is a complicated public policy issue. It is also the subject of continuing litigation.¹⁵ We welcome the opportunity to comment during further consultations on this important related issue.

We note too that the issue of extraterritorial application of Canadian laws must be considered as the proposals in the consultation document may indirectly impact organizations or citizens from other jurisdictions. Again, this is a significant and complex issue in an increasingly globalized economy that involves, for example, many internet service providers and offshore data storage.

Canadian Bar Association.txt

The CBA believes that the quality of any public consultation process is significantly enhanced by the level of detail provided in the consultation documents. To the extent possible it would be helpful to have concepts presented in as much detail as possible, including examples of draft language for the proposals in question.

We look forward to continuing dialogue on these important issues, and thank you again for the opportunity to participate in this consultation.

Yours very truly,

(original signed by Bernard Amyot)

Bernard Amyot

15 See for example R. v. Tele - Mobile, tentatively scheduled to be argued in the Supreme Court of Canada in December of this year.

□