Lawful Access Reform: A Position Paper
Prepared for the
Canadian Association of Chiefs of Police

Prepared by: Lawful Access Subcommittee
CACP Law Amendments Committee
Date: November 2008

Lawful Access Reform: A Position Paper Prepared for the Canadian Association of Chiefs of Police

Introduction

Current lawful access provisions in Canadian law have not kept pace with evolving technology and are inadequate to allow effective access to current and emerging data communications services in Canada. Even when law enforcement and national security have authority to intercept communications, technical barriers can make it practically difficult, even impossible, to effect these court authorized interceptions. This gap between the law and the reality of today's technology poses a serious threat to public safety, creates a safe zone where criminals can operate free from fear of detection and apprehension, and negatively impacts serious criminal investigations, prevention efforts and prosecutions.

The Canadian government, law enforcement, national security, communications service providers, privacy commissioners, and the public agree that changes to legislation are required and that lawful access legislation must balance the privacy of citizens and the capabilities of service providers with the need for law enforcement and national security to access electronic information for legitimate purposes. Opinions on what should be included in those reform efforts, and how they should be rolled out vary considerably between stakeholder groups.

The government introduced Bill C-74, The Modernization of Investigative Techniques Act, in 2006. The bill died on the order paper when Parliament was dissolved. In 2007 the opposition reintroduced the bill as a Private Members Bill which died when Parliament was dissolved in the fall. Although the current government has repeatedly asserted that lawful access reform remains a priority, no legislation has been introduced. The CACP and the CAPB have, over the past 10 years, both adopted several resolutions urging the government to introduce new legislation, and continue to advocate reform.

What is Lawful Access?

Lawful access is a term used in Canada to refer to the interception, search and seizure of communications information by law enforcement and national security agencies pursuant to legal authority provided in the *Criminal Code*, the *Canadian Security Intelligence Service Act*, and other Acts of Parliament such as the *Competition Act.*

The rapid rate of technological expansion and advances in technological capabilities has rendered existing provisions in legislation inadequate to sustain effective interception capabilities. Information technologies such as the Internet, email, cell phones, wireless data networks, voice over internet protocols, wireless e-mail, high speed fiber-optic networks, and encryption add additional layers of complexity and present technical and legal challenges to conventional lawful access methods.

The issue can be divided into several parts:

1. The issue of all telecommunications providers (publicly available services that offer the public means to communicate – telephone companies, ISPs, etc.) being intercept ready. This part of lawful access simply updates the 1974 legislation (i.e. accepts its principles and apply them to today's world);

2. A whole range of search and seizure issues relating to new technologies (i.e. preservation orders and warrants for stored emails in ISPs etc.) and modernization of Part XV of the *Criminal Code* that were discussed but were not part of the lawful access legislation tabled in Parliament;

3. Access to subscriber data (name, address, phone number, email address, etc.). This is not the substance of communications, and the issue becomes when, and under what threshold, should the police be able to access this kind of information.

Why is Lawful Access Reform Important?

Expanded use of technology benefits society, however, it also makes us all more vulnerable. The increasingly global nature of crime increases this vulnerability. Terrorist

groups, pornographers and pedophile networks, illegal traffickers in weapons, drugs and human beings, money launderers and cyber criminals, Internet and telemarketing fraudsters all use technology to develop activities, perpetrate crimes, and avoid detection. Many are using communications technologies that cannot be readily accessed by Canadian law enforcement and national security agencies.

Lawful access legislation and related provisions are valuable tools for law enforcement and national security. Public Safety Canada notes in an Annual Report on Electronic Surveillance (2000) that the conviction rate is over 90% in cases where lawful interception evidence is used in court. The most recent report (2006) highlights that interceptions resulting from lawful authorizations helped lead to the arrest of over 200 criminals in 2006.

Telecommunications carriers have to build into their networks the capacity to respond to court issued access orders. From a law reform perspective, what law enforcement and national security is intercepting is not changing; the authorization process is not changing; but how those warrants are executed is adjusted, to reflect modern realities.

Overview of Lawful Access Reform Legislation in Canada

In August 2002 Justice Canada, the Solicitor General, and Industry Canada issued a Lawful Access Consultation Paper soliciting stakeholder comment on a number of proposals to enhance electronic surveillance powers. The government received over 300 submissions in response to these proposals from the law enforcement community; telecommunications service providers, civil society groups, privacy commissioners, and the public.

A number of submissions were critical of the proposals, arguing that no real justification had been provided for increased government surveillance powers, and that the proposals would unnecessarily and inappropriately curb important civil liberties that are fundamental to a free and democratic society. The CACP disagrees that the core provisions of the lawful access provisions expand surveillance powers. They simply update the existing legislation and recognize that, because of new technologies, communications providers have a greater role in assisting police to implement warrants

that judges have approved. The law enforcement community strongly supported the proposals and urged swift action. The CACP, on behalf of Canadian law enforcement, submitted a comprehensive response, which was supported by over 50 separate letters from individual police agencies and RCMP detachments.

On November 15, 2005 the Liberal Government Minister of Public Safety and Emergency Preparedness introduced Bill C-74, the *Modernization of Investigative Techniques Act*. This bill was introduced a few days before the government was dissolved, and it died on the order paper before any real discussion occurred.

This Act focused on compelling all telephone and Internet companies to create and maintain infrastructures that are intercept capable and to provide access to basic subscriber contact information such as a name, address or telephone number to law enforcement and national security when required to do so. This bill did not introduce Production Orders, Preservation Orders, or other *Criminal Code* amendments as part of the broader package of lawful access proposals on which the government had been consulting.

In brief, the bill required telecommunications service providers to build into their new systems intercept capability to enable law enforcement and national security personnel to intercept communications without facing technical obstacles. Bill C-74 also required telecommunications service providers to respond to warrantless requests by designated law enforcement officials for "subscriber data" (name, address, telephone number, email address, IP address). The bill incorporated a number of safeguards, including many not present in earlier versions of the proposals.

Bill C-74 was also intended as a key step in the harmonization of legislation at the international level. Canada worked with a number of countries to develop the Council of Europe's *Convention on Cybercrime,* developed to foster cooperation internationally and to address global crime and the challenges raised by the expanded use of global communications, which provides a framework for international cooperation. The Convention, which entered into force in July 2004, is the only binding international treaty on the subject effectuated to date. Canada has signed the Convention, but it must now update its legislation to ratify the *Convention* and meet its G8 and other international commitments.

Legislation governing lawful access has already been enacted in the United States (Communications Assistance for Law Enforcement Act, 1994), United Kingdom (Regulation of Investigatory Powers Act, 2000), New Zealand (Telecommunications Interception Capability Act, 2004), and Australia (Telecommunications Interception Act, 1997). Lawful access provisions vary from one country to another, however the stated objectives of each country's Act continues to be to strike a balance between the powers of investigation by law enforcement agencies, the protection of public safety, and protection of privacy.

Canada continues to participate in international discussions on the subject. At the G-8 Justice and Home Affairs Ministerial Meeting in Tokyo in June 2008, Justice Minister Nicholson and Public Safety Minister Day signed the meeting's Concluding Declaration that stated in part:

> *"....we share concerns that the tracking capabilities of law enforcement authorities are falling behind the capabilities of criminals abusing modern communication technologies. Under those concerns, we confirmed that law enforcement authorities should continue to enhance their capabilities so that they can identify and prosecute such criminals anywhere in the world. This year the Roma/Lyon Group has addressed this issue with regard to telecommunications with the goal of sharing beneficial information among the member states. This work has resulted in the recommendation to ensure the closer cooperation between the telephone industry and the law enforcement agencies. We highly value this work and anticipate that law enforcement agencies and the communication industries in each state will work to build a more cooperative relationship. "*

In 2007, additional**,** but more limited consultations by Public Safety Canada and Industry Canada sought comments on the provision of customer name and address information by telecommunications companies to law enforcement and access to email and IP addresses. Bill C-416 (a reintroduction of Bill C-74) was introduced as a Private Members Bill on March 23, 2007, however, died on the order paper when Parliament was dissolved in the fall of 2008. No further legislation has been introduced to date.

Summary of CACP Lawful Access Advocacy and Reform Efforts

The Canadian Association of Chiefs of Police has advocated for over ten years with successive Canadian governments for the creation of a new statute similar to the 2005 *Modernization of Investigative Techniques Act* and accompanying *Criminal Code* amendments. Resolutions adopted by the CACP membership in 1998, 2001, 2003,

2004, and 2007 focused on challenges associated with costs of accessing information, standards, definitions, legislative changes, encryption, and cross border issues.

In addition to adopting these resolutions, the President, Executive Director and other Association executive members have and continue to meet at least once per year with the Ministers of Justice and Public Safety to discuss resolutions which require action. The Law Amendments Committee, the Organized Crime Committee, the National Security Committee, the e-Crime Committee, and the Lawfully Authorized Electronic Surveillance Sub-committee continue their liaison and advocacy efforts at every opportunity. Law Amendments Committee representatives have appeared before Committees of Parliament and the Senate and have intervened in related cases before the Supreme Court of Canada.

Of note is CACP's participation as intervenor in the Supreme Court of Canada case regarding payment of expenses incurred in providing data to police (Tele-Mobile Co. v. Ontario). The Supreme Court 's unanimous decision held that the existing scheme permits ex parte applications for production orders. The Court also concluded that a Judge might only have regard to the financial cost of complying with the production order on a subsequent motion for exemption. Finally, the Court agreed with the decision of the original application judge that an exemption should only be granted if compliance with the production order would be unreasonable. In the circumstances of this case, the Court found that the anticipated cost by Telus of complying with production orders was not unreasonable.

In July 2008, the CACP President sent a letter to the Ministers of Justice and Public Safety stating he was encouraged by their demonstration of commitment to modernizing lawful access legislation by signing of the closing declaration of the G-8 Justice and Home Affairs Ministerial meeting, and further pledged his commitment and resources to assist in introducing lawful access legislation in the next session of Parliament.

Issues

Issues raised in the government's three lawful access consultation processes between 2002 and 2007 are myriad. Law enforcement agencies, the communications industry,

and privacy advocacy groups continue to debate the merits and the downsides of introducing lawful access legislation. A comparative table cross referencing issues and stakeholder groups is attached (Appendix A). The lists of issues presented are by no means exhaustive.

Moving Forward

There appears to be little disagreement among stakeholders that Canadian legislation must be amended to reflect changes in technology. Perspectives on what should be included in those reform efforts, and how they should be rolled out vary considerably between stakeholder groups. The CACP's investment in bringing this complex, multi-faceted, and controversial issue to the government's attention has been significant. However, repeated attempts by the CACP and others to urge the government to introduce reforms have not yielded the desired results.

The CACP views lawful access reforms as an essential ingredient in their commitment to the continued provision of quality police services that enhance Canadian public and community safety and security. To that end, it is incumbent on the CACP to educate the public about the significant issue involved, and to compel the government to action in order to preserve and safeguard the safety of all Canadians.

Appendix #1

Lawful Access Issue Comparisons

Issue	CACP & Law Enforcement	Communications Industry	Public	Privacy Commissioners
New legislation required	Agreed	Agreed	Agreed somewhat – updates required	Agreed
Harmonization with international standards	Legislation required			
Communication service provider capability and capacity to provide subscriber and service provider information	Legislation required	Opposed to being obliged to collect, maintain or guarantee the accuracy of subscriber information beyond what is required for their own business purposes	Concern that increased surveillance will create opportunities for abuse by police and service providers	
Requirement to provide subscriber and service provider information	Legislation required or authorization to use production orders		Job of service providers is to proved service for customers; not monitoring customers for purposes of the state.	
Collection of communications traffic data	Legislation required			
Communications content and related traffic data	Access required			
Forbearance	Exception rather than the rule			
Communications service provider infrastructure cost recovery	Should not be recovered from law enforcement or national security agencies		Concerned that communications service customers will have to bear costs	
Access capability to new or upgraded technologies	Costs to be borne by communications service providers	Government should pay until solutions can be deployed and maintained at minimal incremental cost		
Costs associated with provision of court ordered assistance	Costs to be borne by communications service providers	Law enforcement agencies should bear reasonable costs. Also concerned about costs of staffing 24/7	Concerned that communications service customers will have to bear costs	
Nationally standardized costs	Yes	Costs should be negotiated between individual service providers and agencies		

Lawful Access Issue Comparisons

Issue	CACP & Law Enforcement	Communications Industry	Public	Privacy Commissioners
Production orders	Yes. Criminal Code amendment required		Require information on differences between production orders and search warrants	
Basic subscriber and service provider national database	Yes. Federally funded. Legislation required.	Opposed – concerned about privacy, security and high costs of development		Opposed
Data preservation	Legislation, processes and procedures required		Require information on differences between data preservation and data retention	
Computer viruses	Legislation required to make it an offence to possess, create, or sell			
Email	Interception and seizure must be clarified. Legislation required.	Interception of unviewed email and other communications traffic in transit should be considered private communication and should require a search warrant or production order to access		
Video interception must be done by police officer	Amend legislation to read "*person acting under direction of a police officer*"			
Part VI interception orders specify location	Not applicable to wireless services. Amendments to legislation required.			
Live monitoring where call block facilities available	Criminal code amendment required to dispense			
Pre-paid or pay as you go communications services	Require regulatory obligations to identify users			Vehemently opposed – viewed as a gross invasion of privacy
Wireless and satellite cross border intercepts	Legislative amendment and expedited procedures and agreements required			
Technology that precludes lawful interception	Prohibition required			

Lawful Access Issue Comparisons

Issue	CACP & Law Enforcement	Communications Industry	Public	Privacy Commissioners
Invasion of privacy			Significant concern	
Expansion of police powers			Significant issue for monitoring of online communication without judicial authorization	
Increased ease of law enforcement access to private communications and subscriber data			Significant issue	
Retention, use, and disclosure of communications data gathered			Significant concern	General data retention requirements should not be part of any lawful access initiative
Safeguards to protect against abuse			Inadequate	
Oversight mechanisms			Inadequate	
Justification			Insufficient for measures being proposed	Looking for more clarity on why proposed measures are necessary
Benefit			Has not been demonstrated	
Fighting organized crime and terrorism			Linkages have not been clearly defined	
Variability in standards			Interception standards for telephone, on line communication and postal mail should be the same	Email should have same standard of protection as phone calls and letters. Users need confidence that their online communications and activities will not be arbitrarily intercepted or scrutinized
Definitions	Legislative amendment required to encompass emerging technologies	Terms require clarification		
Harmonization with international legislation		Canadian definitions must be consistent with internationally used definitions		If Convention calls for unjustifiable intrusion on the privacy, inconsistent with Canadian values and rights, the Convention should not be ratified.
Encryption	Comprehensive legislation required			

Lawful Access Issue Comparisons