Lawful Access – Consultation Document

Department of Justice
Industry Canada
Solicitor General Canada

August 25, 2002

Government of Canada Gouvernement du Canada

Canada

Table of Contents

INTRODUCTION 3
A Rapidly Evolving Environment 3
The Council of Europe *Convention on Cyber-Crime* 5
Public Policy Objectives 5
The Consultation Process 6
LEGISLATIVE PROPOSALS 7
Infrastructure Capability 7
Requirement to Ensure Intercept Capability 7
General Requirements 8
Regulations 8
Forbearance 9
Compliance mechanism 9
Costs of Ensuring Intercept Capability 9
Amendments to the *Criminal Code* and other statutes 10
Production orders 10
General production orders 10
Specific production orders 11
Orders to obtain subscriber and/or service provider information 12
Assistance orders 13
Data-preservation orders 13
Virus Dissemination 14
Interception of e-mail 15
Amendments to the *Competition Act* 17
Other mechanisms to provide subscriber and service provider information 17
CONCLUSION 19
Appendix 1: Interception 20
Appendix 2: Search and Seizure 21

INTRODUCTION

Lawful Access is an important and well-established technique used by law enforcement and national security agencies to conduct investigations. In the context of telecommunications in Canada, it consists of the interception of communications and search and seizure of information carried out pursuant to legal authority as provided in the *Criminal Code*, the *Canadian Security Intelligence Service Act,* and other Acts of Parliament such as the *Competition Act*. These Acts provide law enforcement and national security agencies with powers to intercept communications and search and seize information in a manner consistent with the rights and freedoms guaranteed in the *Canadian Charter of Rights and Freedoms*, particularly the right to be secure against unreasonable search and seizure. (Further details regarding interception and search and seizure can be found in, respectively, Appendix 1 and Appendix 2.)

For law enforcement and national security agencies, lawful access is an essential tool in the prevention, investigation and prosecution of serious offences and the investigation of threats to the security of Canada. Lawfully authorized interception and the search and seizure of documentation, computer data, and other information is used frequently by law enforcement agencies to investigate serious crimes such as drug trafficking, child pornography, murder, money laundering, price fixing and deceptive telemarketing. National security agencies utilize lawfully authorized interception to investigate terrorist and other threats to national security. According to the *Solicitor General's Annual Report on the Use of Electronic Surveillance*, the conviction rate is in excess of 90% in those cases where lawful interception evidence is used or adduced in court.

Clearly, it is important to maintain the principle and powers of lawful access. The challenge is to do so in the face of rapid technological change and in a manner consistent with the *Canadian Charter of Rights and Freedoms*.

A Rapidly Evolving Environment

Modern telecommunications and computer networks such as the Internet are a great source of economic and social benefits, but they can also be used in the planning, coordination, financing and perpetration of crimes and threats to public safety and the national security of Canada.

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

While providers of certain wireless services, such as Personal Communications Services, have since 1996 been required to have facilities capable of lawful access pursuant to a licensing obligation under the *Radiocommunications Act*, there are currently no similar obligations for other providers.

Working Definition

"Service Provider" means a person who owns or operates a transmission facility that is used by that person or another person to provide telecommunications services to the public in Canada.

The new competitive telecommunications market has seen many new entrants along with new services offered using new technologies, and these often raise problems for lawful access. Today, wireline providers are joined in the communications market by a variety of wireless providers and a large number of Internet service providers, resulting in a complex environment in which law enforcement and national security agencies must carry out their investigations.

A number of technological developments that affect lawful access have emerged in recent years. These include:

Wireline communications: Law enforcement and national security agencies have conducted lawful investigations with the assistance of wireline service providers for many years. However, advanced service options and calling features have created new challenges for investigators.

Wireless communications: The rapid expansion in the use of wireless communication devices like cellular telephones, digital wireless phones such as Personal Communications Services and satellite-based communications can pose significant challenges if the infrastructure supporting these devices does not include lawful access capabilities. The rate at which new wireless technologies and services are introduced in the marketplace makes it very difficult for law enforcement and national security agencies to sustain their technical ability to lawfully intercept communications. Moreover, the global nature of these technologies can create significant jurisdictional problems in criminal and terrorist investigations.

The Internet: The Internet is an amalgamation of over 135,000 networks around the world, all of which operate using packet switching and can exchange and share information. This "network of networks" has no centralized physical location or control. The technology used for Internet communication, the need for sophisticated equipment to lawfully intercept Internet communications and the lack of provisions that would require Internet service providers to implement procedures for lawful intercept capabilities, have created difficulties for investigators.

As information and communications flow more easily around the world, they also challenge existing legal provisions, agreements and techniques. Borders are no longer boundaries to this flow, and criminals are increasingly located in places other than where their acts produce their effects. In the face of these developments, law enforcement and national security agencies need modern and effective capabilities to support their investigative or intelligence gathering efforts. Legislative proposals are being considered to bring the law into accordance with the current state of telecommunications technology. To contribute to the development of this legal framework, and to help law enforcement and national security agencies navigate this new environment, partnerships with Canadian industry are more important than ever and must be consistently fostered and maintained.

The Council of Europe *Convention on Cyber-Crime*

The Council of Europe *Convention on Cyber-Crime* is an international treaty that provides signatory states with legal tools to help in the investigation and prosecution of computer crime, including Internet-based crime, and crime involving electronic evidence. As a permanent observer to the Council of Europe, Canada was invited to participate in the negotiation of the *Convention*. As of August 2002, 33 countries had signed the C*onvention*, including Canada and most of its G8 partners.

The *Convention* calls for the criminalization of certain offences relating to computers, the adoption of procedural powers in order to investigate and prosecute cyber-crime, and the promotion of international cooperation through mutual legal assistance and extradition in a criminal realm that knows no borders. The *Convention* will help Canada and its partners fight crimes committed against the integrity, availability and confidentiality of computer systems and telecommunications networks and those criminal activities such as online fraud or the distribution of child pornography over the Internet that use such networks to commit traditional offences. Most of the required offences and procedures already exist in Canada. However, before Canada can ratify the *Convention* and give it effect, the *Criminal Code* would need to be amended to include:

- provisions for a production order;
- provisions for a preservation order; and
- an offence in relation to computer viruses that are not yet deployed.

Complementary or further amendments could be made to other existing laws, such as the *Competition Act*, in order to modernize them in accord with the *Convention*, notably in the areas of real-time tracing of traffic data (see section on Specific Production Orders below) and interception of e-mail.

Proposals regarding these amendments are outlined and explained below.

Public Policy Objectives

The Government's approach recognizes the need for effective measures that balance the rights, privacy, safety, security and economic well being of all Canadians. To realize their public safety mandates, law enforcement and national security agencies need to maintain their lawful access capabilities in a manner that continues to respect the *Canadian Charter of Rights and Freedoms*.

Consistent with the pledge in the 2001 Speech from the Throne to provide modern tools to deal with cyber-crime, these proposals are intended to update the existing legal framework to help law enforcement and national security agencies address the challenges posed by advanced communications and information technologies.

The public policy objectives of this process are to maintain lawful access capabilities for law enforcement and national security agencies in the face of new technologies and to preserve and protect the privacy and other rights and freedoms of all people in Canada. In striving to attain these goals, it is essential to ensure that no competitive disadvantages are placed on Canadian industry and that the solutions adopted do not place an unreasonable burden on the Canadian public.

The Consultation Process

The Department of Justice Canada, in collaboration with the Portfolio of the Solicitor General of Canada and Industry Canada, are examining the various options available to address the challenges posed to lawful access in the context of modern telecommunications technology and are carrying out consultations to inform their efforts.

The purpose of this document is to provide a range of stakeholders, including the provinces and territories, law enforcement and national security agencies, telecommunications and related industry representatives, civil liberties organizations and the legal community, with an opportunity to consider proposals to update Canada's lawful access provisions. The proposals address requirements stemming from three primary needs: (1) the need to bring the provisions of the law into concordance with new telecommunications technology; (2) the need for all telecommunications service providers to ensure that the technical capability in their facilities permits lawful access by law enforcement and national security agencies; and (3) the need for Canada to adopt statutory measures that will permit ratification of the Council of Europe *Convention on Cyber-Crime*.. These proposals are the result of a comprehensive legal review that began in October 2000.

The proposals in this document are points of departure for discussion and input on any or all of the proposals is welcomed.

LEGISLATIVE PROPOSALS

The following proposals address the requirement for service providers to provide the technical capability for lawful access, as well the need to bring the *Criminal Code* in line with new telecommunications technology and make necessary amendments to the *Criminal Code* and other statutes, such as the *Competition Act*, that would allow Canada to ratify the Council of Europe *Convention on Cyber-Crime*.

Several of Canada's international partners have already updated their legislation to ensure that their law enforcement and national security agencies maintain their lawful access capabilities. Modernizing our legislative framework is needed for Canada to continue to be an effective partner internationally and to address the challenges posed by the current state of telecommunications technology.

Infrastructure Capability

Requirement to Ensure Intercept Capability

There is currently no legislative mechanism in Canada that can be used to compel service providers to develop or deploy systems providing interception capability, even if a legal authorization is obtained by law enforcement or national security officials to intercept the communications of a specific target.

It is proposed that all service providers (wireless, wireline and Internet) be required to ensure that their systems have the technical capability to provide lawful access to law enforcement and national security agencies. The implementation and maintenance of this capability is the focus of this section.

Working Definition
"Transmission Facility" means any wire, cable, radio, optical or other electromagnetic system, or any other (similar) technical system, used for the transmission of information between network termination points.

The central tenet of the proposal is that service providers would be required to have the technical capability to provide access to the entirety of a specific telecommunication transmitted over their facilities, subject to a lawful authority to intercept. This would include the content and the telecommunications-associated specific data associated with that telecommunication.

A new law addressing the requirement for service providers to have intercept-capable transmission apparatus could set out the following:

- general operational requirements describing the interception capability;
- regulation-making authority to specify the details of the functional requirements;
- a capacity for forbearance from certain obligations; and

- a compliance mechanism.

General Requirements

The legislation would apply to all service providers operating a telecommunications facility in Canada. All service providers would be required to provide, at a minimum, a basic intercept capability before providing new services or a significantly upgraded service to the public. The requirements of the legislation would come into effect as of a date to be proclaimed by the Governor-in-Council (Cabinet).

Regulations

It is crucial that service providers know what is required of them. The legislation would set out the definitions and the general approach and would provide authority for the Cabinet, on the advice of the Minister of Industry and the Solicitor General, to make regulations within the authority provided in the statute. Technical standards and details could be specified in the regulations.

The scope of the regulations is open to discussion but could include authority relating to the setting of technical and other standards or requirements for a service provider. Regulations could describe what service providers must do to provide access to their facilities, security requirements relating to how intercepted information is handled, issues related to costs, and the manner in which the regulations are to be developed.

Issues to be considered

1. how could regulations prescribe technical and other standards or requirements for:
    a. apparatus to be installed, attached or otherwise related to its facility, and the capacity requirements for the maximum number of simultaneous interceptions pertaining to such apparatus?

Working Definition

"Transmission apparatus" means any apparatus that is used for

a) the switching of information transmitted by telecommunication;
b) the input, capture, storage, organization, modification, retrieval, output or other processing of information transmitted by telecommunication; or
c) control of the speed, code, protocol, content, format, routing or similar aspects of the transmission of information by telecommunication

    b. terms and conditions pertaining to the security of interceptions and of the delivery of the product of interceptions?

    c. the competence, reliability and deployment of employees?

2. should regulations provide for fees to be paid to a service provider for operational assistance?

Before recommending any regulation to Cabinet, the Minister of Industry and the Solicitor General would consult with appropriate persons representing the interests of those affected by the regulations.

Forbearance

Since the requirement to ensure intercept capability would apply to all service providers, the legislation needs to be flexible and able to adapt to special situations. One mechanism to provide flexibility and avoid problems such as the creation of "intercept safe-havens" would be a system of forbearance. This forbearance would remove the obligation to comply with the requirements of the statute or regulations, in whole or in part, for a limited time.

The way by which forbearance may work, for example, is that the Cabinet would have the authority to forbear but would delegate this authority jointly to the Solicitor General and the Minister of Industry. Administrative guidelines would be prepared by the two departments to govern their management of requests for forbearance, and those guidelines would be made publicly available. During the period when the Ministers are considering a request for forbearance, the service provider would not be subject to penalty.

Compliance mechanism

Provisions for monitoring compliance would help ensure that the legislation is effective and that service providers have a mechanism to help ascertain compliance with the law. The provisions could authorize or require inspections or analyses to be conducted. However, these mechanisms would need to minimize the costs for both industry and government.

Issues to be considered

- what kind of compliance mechanism should be established?
- who should conduct the compliance activities and prescribe the circumstances under which they may be conducted?
- what type of penalty should be provided for in cases where service providers do not comply with the law?

Costs of Ensuring Intercept Capability

The government is exploring how costs could be allocated within a regime that covers three main sets of circumstances. As of a date to be proclaimed by Cabinet:

1. service providers would be responsible for the costs associated with providing the lawful access capability for new technologies and services, and
2. service providers would be responsible for the costs associated with providing a lawful access capability when a significant upgrade is made to their systems or networks, however
3. they would not be required to pay for necessary changes to their existing systems or networks.

Amendments to the *Criminal Code* and other statutes

Several amendments to the *Criminal Code* have been proposed to deal with the interception and search-and-seizure provisions noted above, and to permit Canada to ratify the Council of Europe *Convention on Cyber-Crime*.

Production orders

A production order requires the custodian of documents to deliver or make available the documents to persons such as law enforcement officials within a specified period. Production orders already exist in some federal laws, such as the *Competition Act*. However, except for a very narrow type of production/collection orders, there are currently no production orders provided for in the *Criminal Code.*

In order to give law enforcement agencies appropriate procedural powers to deal with new technologies, three legislative proposals are under consideration:

- create a general production order;
- create a specific production order for traffic data;
- create a specific production order for subscriber and/or service provider information.

If either a specific or a general production order is created, it is essential to recognize and maintain rights protected by the *Canadian Charter of Rights and Freedoms*, such as protection to individuals against self-incrimination.

General production orders

In some cases of searches against third parties, such as corporations or banks, law enforcement agencies obtain judicial search warrants but do not actually conduct the searches themselves. For practical reasons, the third-party custodian of the documents is often in a better position to produce the documents. However, it can take some time for that third party to find and produce the documents for law enforcement agencies.

One way of solving this problem could be to create a general production order requiring the custodian to deliver or make available the documents to law enforcement officials within a certain period of time. A production order could be issued in circumstances similar to those under which a search warrant is issued. Executing such an order might be considered less intrusive than a search warrant as there would be no entry into and search by law enforcement agencies of the premises of the third party. Such production orders could also allow law enforcement officials to obtain documents in cases where a search warrant cannot be delivered because the documents are stored in a foreign country.

Issues to be considered

- should the *Criminal Code* be amended to allow law enforcement officials to obtain production orders in specific cases?
- should the *Criminal Code* allow for anticipatory orders (e.g., permit law enforcement agencies to monitor transactions for a specified period of time)?
- what kind of procedural safeguards should be included?

Specific production orders

The *Criminal Code* generally provides that law enforcement agencies cannot obtain documents or information without having reasonable grounds to believe that an offence has been or will be committed. This requirement is a safeguard that balances the state's need to obtain evidence of a crime with the privacy interests of a person holding information. This requirement is particularly appropriate where there is a high expectation of privacy, such as in regard to the content of a private document. However, the *Criminal Code* also provides for production/collection orders under a lower standard in a very limited number of cases, such as income tax information for specific offences, tracking devices and dial number recorders (devices that record incoming and outgoing telephone numbers), at an earlier stage of the investigation. Except in these very limited cases, the current safeguard prevents important information from being gathered at an early investigation stage, even if there is a low expectation of privacy in relation to the information being sought.

Working Definition

"Telecommunications Associated Data" means any data, including data pertaining to the telecommunications functions of dialling, routing, addressing or signalling, that identifies, or purports to identify, the origin, the direction, the time, the duration or size as appropriate, the destination or termination of a telecommunication transmission generated or received by means of the telecommunications facility owned or operated by a service provider.

A specific production order could be created under a lower standard in order to allow for the production of telecommunications associated data, that extends beyond the telephone numbers already covered by section 492.2 of the *Criminal Code*, historic traffic data or real-time collection of traffic data. Although real-time search of traffic data is already permissible under either section 487.01 or Part VI, the standard for Internet traffic data should be more in line with that required for telephone

records and dial number recorders in light of the lower expectation of privacy in a telephone number or Internet address, as opposed to the content of a communication.

A specific production order to be issued under a lower standard could also be created to obtain other data or information in relation to which there is a lower expectation of privacy.

Issues to be considered

- should there be a specific power, parallel to that provided for in the *Criminal Code* dial number recorders, to allow law enforcement and national security agencies to obtain traffic data?
- how should "traffic data" be defined? Should the definition of traffic data be combined with telephone-related information and addressed in the same *Criminal Code* provision?
- should other specific production orders be created under a lower standard?
- what kind of procedural safeguards should be included?

Orders to obtain subscriber and/or service provider information

Basic customer information such as name, billing address, phone number and name of service provider, has historically been made available by service providers without a prior judicial authorization (such as a search warrant). For instance, the Supreme Court of Canada decision in *R. v. Plant,* (1993) 3 S.C.R. 281, held that, in the context of information held by a business, a person does not have a reasonable expectation of privacy in personal information that does not tend to reveal intimate details of his or her lifestyle and personal choices. The *Personal Information Protection and Electronic Documents Act* allows for the disclosure of personal information without the knowledge and consent of the individual to whom it pertains, as long as that disclosure is requested by a government institution that has identified its lawful authority to obtain such information.

In addition, in relation to Customer Name and Address (CNA) information, the Canadian Radio-television and Telecommunications Commission (CRTC) decided that it would not exert its jurisdiction in relation to such information if it was confidential, and is currently considering whether some service providers might conduct reverse searches on non-confidential customer name and address information. Further to recent rulings by the CRTC, information that identifies a local service provider can only be provided if certain specific conditions have been met.

However, if such conditions have not been met or if the custodian of the information is not cooperative, law enforcement agencies have no means to compel the production of information pertaining to the customer or subscriber without some form of court order. A problem does exist in cases where no warrant can be obtained under the *Criminal Code* (e.g., s. 487) because 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.

Issues to be considered

- should there be a specific production order in relation to customer name and address and service provider information?
- under what conditions should such information be made available and to whom?
- what is the standard that should be required?
- should this obligation be imposed even if the service provider is not currently collecting this information for its own purposes?

Assistance orders

Section 487.02 of the *Criminal Code* provides that a judge or justice who gives an authorization to intercept a private communication, who issues a search warrant or who makes an order authorizing the use of a dial number recorder may also make an order requiring any person to assist in the execution of these orders. Such assistance orders may only be issued where the person's assistance may reasonably be required to give effect to these orders.

Some law enforcement officials have raised the possibility of including assistance orders in other acts, such as the *Competition Act*, that already allow for the issuance of search warrants or for the granting of interception authorizations. Some stakeholders have also suggested that any *Act* allowing for the issuance of assistance orders should spell out what could specifically be required under such orders. In the context of lawful access such clarifications in the law could allow service providers to understand more clearly the extent of their obligations.

Issues to be considered

- should legislation that already allows for the issuance of search warrants or the granting of interception authorizations be amended to include the possibility for a judge or justice to issue an assistance order to give effect to the warrant or authorization?
- should assistance orders more clearly spell out the scope and limits of what a person may be required to do to give effect to the warrant or authorization?

Data-preservation orders

A procedural mechanism in the Council of Europe *Convention on Cyber-Crime* that does not exist in Canadian law is the concept of a preservation order. A preservation order acts as an expedited judicial order that requires service providers, upon being served with the order, to store and save existing data that is specific to a transaction or client. The order is temporary, remaining in effect only as long as it takes law enforcement agencies to obtain a judicial warrant to seize the data or a production order to deliver the data. For

example, a preservation order could require an Internet service provider (ISP) not to delete specific existing information relating to a specific subscriber. It is meant as a stop-gap measure to ensure that information vital to a particular investigation is not deleted before law enforcement officials can obtain a search warrant or production order.

Consideration also needs to be given to exigent circumstances, situations in which it could be argued that law enforcement agencies should be able to impose on a service provider the requirement to preserve data even without a judicial order for a specified period such as four days, if the conditions for obtaining a judicial order exist but it would be impracticable to obtain one. An exigent circumstance provision is already included in the *Criminal Code* in relation to search warrants and wiretaps.

It should be noted that data preservation is different from data retention. Data preservation, as outlined above, involves serving a judicial order on a service provider to *ensure that existing specified information in relation to a particular subscriber is not deleted*. Data retention, however, is a general requirement that could compel service providers to *collect and retain a range of data concerning all of its subscribers*.

Issues to be considered

- should a data-preservation order apply only to stored computer data or should it also apply to paper records?
- under what legal standard should a data-preservation order be granted?
- should standards vary depending on the nature of the data?
- who should be authorized to issue a preservation order?
- what is a reasonable period for a custodian of data to be compelled to preserve data: 90, 120, 180 days?
- should there be a specific penalty for non-compliance with a preservation order, or is contempt of court sufficient?
- for how long should a law enforcement official be able to impose a preservation order on service providers in exigent circumstances?

Virus Dissemination

Under the current provisions of the *Criminal Code*, only the effects of spreading a computer virus, or an attempt to do so, are criminal acts. In 1985, when the provisions on unauthorized use of computers were enacted, complementary changes were also made to the *Criminal Code* provisions relating to mischief to ensure that any type of behaviour involving a computer system which amounted to mischief would be criminal acts under Canadian laws.

The Council of Europe *Convention on Cyber-Crime* requires signatory states to criminalize the creation, sale and possession without right of devices (e.g., computer programs) that are designed or primarily adapted for the purpose of committing offences specified in the *Convention*, whether or not the virus has been deployed or has caused any form of

mischief. Such a distinction is not included in the current wording of the *Criminal Code*. A minor change in the wording of section 342.2 would be necessary to clarify that the creation, sale and possession of a computer virus program for the purpose of committing a computer offence or mischief is an offence in Canadian law.

Further, in order to ratify the *Convention*, new offences in relation to illegal devices (such as viruses) would have to be added. These could include importation, procurement for use, and otherwise making available an illegal device as defined in the *Convention*.

Interception of e-mail

Part VI of the *Criminal Code* creates an offence for wilfully intercepting a "private communication", as well as a scheme for obtaining judicial authorization to intercept such communications. (See Appendix 1 for a description of the current interception provisions in the *Criminal Code.)* The requirements for intercepting a "private communication" are more onerous than those required to obtain a search warrant to seize documents or records (See Appendix 2). Section 183, in Part VI of the *Criminal Code,* defines the expression "private communication" to cover any *oral* communication, or any telecommunication made under circumstances creating a reasonable expectation of privacy. This appears to suggest that, once a communication is put in writing, it can no longer be considered a "private communication" for the purpose of the interception of communications provisions of the *Criminal Code*.

In fact, some courts have held that a tape-recorded message, like a written letter, did not fall within the definition of "private communication" because it was not reasonable for a person sending such a tape (or letter) to expect that it would remain completely private. As it was a permanent record of its contents, it could easily come into the hands of a third party. Following this line of reasoning, one could argue that e-mail communications, as they are in writing, would not come within the "private communication" definition. Therefore, these written records could be obtained by a search warrant.

However, some cases dealing with e-mails in Canada have taken the position that they are to be considered "private communications." For example, a judge in Alberta recently held that judicial authorization under Part VI was required to intercept e-mails since there was a reasonable expectation of privacy on the part of those sending and receiving them.

These decisions, along with the definition of “private communication,” create some confusion as to whether an e-mail should be seized or intercepted. The problem stems from how this “store and forward” technology works. It is in fact possible to access an e-mail in various places or at various stages of the communication or delivery process using various techniques. The following stages of the communication or delivery process could probably be qualified as “interceptions”:

- during keyboarding on the part of the sender of the message
- during transmission between the sender’s computer and the sender’s ISP
- during transmission from the sender’s ISP to the recipient’s ISP

- during transmission between the recipient's ISP and the recipient's computer
- during reception by the recipient of the sender's message

The way e-mail messages are transmitted, the relationship between the transmission and/or reception of the message, and the interplay between the sender and the recipient would appear to be covered by the current definition of the term "intercept" in the *Criminal Code*.

Two stages are more problematic:

- while e-mail is stored at the sender's ISP
- while e-mail is stored at the recipient's ISP

The acquisition of e-mails under these circumstances can on occasion be at the same time as the transmission of those e-mails, but it may also be delayed. Additionally, e-mails may be stored for long periods (weeks or months) before they are opened by the recipient. The simultaneous transmission and acquisition of the content of an e-mail could be similar to an "interception" under Part VI the *Criminal Code*. However, the acquisition of those contents when they are stored could also be considered a "seizure" under Part XV of the *Criminal Code* or, for example, under s.15 or 16 of the *Competition Act.*

One final situation also raises problems: seizing an opened e-mail at the recipient's ISP.

This stage is similar to the situation where a person, having read a letter, files it into a filing cabinet rather than throwing it into the garbage. Obtaining an e-mail at this stage is more analogous to a seizure than it is to an interception.

The main problem in Canada is that the capture of the contents of an e-mail in transit with a third party or waiting to be delivered could constitute an "interception" of a "private communication" under the *Criminal Code*, regardless of when it took place. Some claim, however, that the acquisition of an e-mail under such circumstances constitutes a "search and seizure." Questions have been raised as to whether the *Criminal Code* and other acts such as the *Competition Act* should be amended to clarify the type of order that should be obtained before e-mail is acquired.

Issues to be considered

- should there be a specific provision in the *Criminal Code* in relation to how an e-mail should be acquired?
- if such a provision should be included, what kind of procedural safeguards should be imposed?
- should the type of order to be obtained in order to acquire an e-mail vary depending on the stage of the communication or delivery process?

Amendments to the *Competition Act*

In addition to identified needs similar to other law enforcement agencies, such as proposed amendments relating to data-preservation orders and orders to obtain subscriber and/or service provider information, discussed above, the Competition Bureau is facing significant new technology-related challenges that impact on its capacity to obtain lawful access to evidence of *Competition Act* offences.

Deceptive marketing practices, telemarketing and other consumer targeted fraud, price fixing and bid-rigging are some of the competition offences that can be facilitated by computer systems and telecommunications. The nature of evidence for these kinds of offences is now increasingly electronic and significant amounts of data can be stored on increasingly smaller devices or media. Additionally, the type of criminals associated with some of these crimes is evolving. In telemarketing, for example, aliases are frequently used and there is a growing link between criminal elements associated with this kind of activity and threats to the security of Canadians.

Investigative powers currently available to the Competition Bureau include production orders, search and seizure, and interception of private communications. In order to continue to be able to legally access the type of evidence needed to fulfill its mandate, it has been proposed that amendments to the *Competition Act* should be considered, such as:

Access to Hidden Records

This proposal involves the capability of requesting persons found on a search premises to provide any records hidden on their person, including hidden electronic and digital devices or media mentioned in the search warrant, to officers on the premises; and provide for an obstruction provision specific to those failing to comply.

Other Orders

This proposal involves the ability to obtain general warrants and assistance orders to enhance the efficacy of evidence gathering tools.

Other mechanisms to provide subscriber and service provider information

Law enforcement and national security agencies require accurate information on the subjects of their investigations in order to determine where to target an interception. Law enforcement agencies also require such information to obtain a search warrant.

With deregulation of the telecommunications market, the telephone network has become so complex that law enforcement and national security agencies are experiencing delays and difficulties in identifying the local service provider. Determining the local service provider identification (LSPID) information is the first step in identifying a subscriber by

means of address or telephone number. However, the only way in which this information can be obtained is through the time-consuming and costly process of directly contacting each local carrier.

The CRTC recently approved the conditions under which Bell Canada could release LSPID (http://www.crtc.gc.ca/archive/ENG/Decisions/2002/dt2002-21.htm) information without a court order for emergency, national security and law enforcement purposes. The LSPID service to be provided by Bell Canada would alleviate some of the concerns expressed by law enforcement in particular about obtaining access to accurate and timely information.

A related issue is how law enforcement and national security agencies can obtain access to customer name and address information, bearing in mind that some service providers do not even collect or store such information. The CRTC decided that it would not exert its jurisdiction over information pertaining to confidential customer name and address. It is also currently considering whether some wireline providers may conduct reverse searches on non-confidential customer name and address information.

Some states, such as Australia, the Netherlands and Germany, have established databases or statutory means for law enforcement and national security agencies to obtain accurate subscriber and service provider information more quickly. In these countries, telecommunications service providers are required to provide such information and are responsible for its accuracy, completeness and currency.

The Canadian Association of Chiefs of Police has made recommendations to improve lawful access to this information, including the establishment of a national database. The implementation of such a database would presuppose that service providers are compelled to provide accurate and current information. Other options, including the use of existing sources of information such as provincial 911 databases or private telephone directories, may be appropriate. Any such option would need to be used in a way that is consistent with the *Privacy Act*, the *Personal Information Protection and Electronic Documents Act*, and any other applicable laws.

Issues to be considered

- what type of mechanism, if any, should be put in place to provide law enforcement and national security agencies with up-to-date and accurate CNA and LSPID information while respecting the privacy of Canadians?
- should an obligation to collect such CNA information be imposed even if the service provider does not collect this information for its own purposes? In other words, should a provider be compelled by law to collect CNA information?
- some mechanisms with respect to CNA information are already in place with respect to telephones. Should such mechanisms be created or adapted to provide similar subscriber information for Internet service providers?
- who should pay the costs of collecting, retaining and accessing this information?
- if a database were to be established, who should operate this database?

CONCLUSION

Government of Canada officials expect to meet with a variety of interested parties in the fall of 2002 to discuss the issues raised in this paper. Your input is welcome and it will assist the Government of Canada in developing an appropriate response to these issues.

This and other documentation related to the consultation is available online at the Department of Justice Internet site located at http://www.canada.justice.gc.ca/en/cons/la_al. Comments may be provided by email to la-al@justice.gc.ca or by using the email link on the department's Internet site. Comments may also be provided by mail to

Lawful Access Consultation,
Criminal Law Policy Section
5th Floor,
284 Wellington St.,
Ottawa, Ontario, Canada, K1A 0H8.

All comments should be submitted by November 15, 2002, so that they can be taken into consideration.

Appendix 1: Interception

The provisions of what is now Part VI of the *Criminal Code* came into force over 28 years ago, on July 1, 1974. These provisions protect the privacy of Canadians by making it an offence to intercept private communications except where permitted by law, while providing the police with the means to obtain judicial authorizations to assist in criminal investigations. The requirements for granting an authorization under section 185 and a warrant under section 487.01 are described in Parts VI and XV of the *Criminal Code*.

The following are the key features of these requirements:

- a police investigator must swear an affidavit deposing to the facts relied upon to justify the belief that an authorization or warrant should be given, and provide reasonable grounds to believe that electronic surveillance of certain persons or the search of certain locations may assist in the investigation of the offence.

- the designated agent is responsible for ensuring that all matters relating to the application comply with the law. In addition, the agent must ensure that the offence is of a serious enough nature to warrant the application and that there is not already sufficient evidence to prove the offence.

- in the case of a section 185 application, the judge must be satisfied that granting the authorization would be in the best interests of the administration of justice, and that other investigative procedures have been tried and have failed, or other investigative procedures are unlikely to succeed or the matter is so urgent that it would be impractical to carry out the investigation using only other investigative procedures. The latter requirements do not apply in limited circumstances relating to criminal organizations. The judge may also impose such terms and conditions on the implementation of the authorization, as the judge considers appropriate.

The following are the key features of the section 185 procedural regime:

- only the Solicitor General, or persons specially designated by the Solicitor General, may make an application for an authorization in relation to offences that would be prosecuted on behalf of the Government of Canada. In practice, applications for authorizations are made by lawyers employed by or under contract with the federal Department of Justice who are designated by the Solicitor General. Senior police officers are also specially designated by the Solicitor General in the case of emergency authorizations.

- law enforcement officers may request that the designated agent make an application only after receiving the written approval of a senior officer in their respective law enforcement agency.

Appendix 2: Search and Seizure

A search is the investigation of a place in order to discover something or to search for evidence of a breach of a law to be used in criminal or penal proceedings. When it happens in the course of a search, a seizure may be defined as a "seizure of property for investigatory or evidentiary purposes."

The element that underlies these two definitions is that of active scrutiny, generally for penal purposes. Powers of inquiry, investigation and seizure imply a systematic scrutiny by a public servant who, having reasonable grounds to believe that there has been a breach of the law, is looking for evidence of the offence. Such scrutinizing is undertaken for the purposes of suppressing violations of the law and punishing those who break it.

Except in exceptional circumstances, such as in cases in which a warrant cannot be obtained because it would be impractical to obtain it by reason of exigent circumstances, searches and seizures are conducted under the authority of a search warrant obtained generally, in the context of the *Criminal Code,* under s. 487 or 487.01, or the *Competition Act*, under s.15 or s.16. The issuance of a search warrant is a judicial act on the part of a justice, usually performed *ex parte* and *in camera,* by the very nature of the proceeding. A search warrant authorizes a peace officer or a public officer to search a building or place, or a computer system in a building or place for anything that will afford evidence of an offence and seize it.

The decision of the Supreme Court of Canada in *Hunter* v. *Southam* makes it clear that, *prima facie*, a warrantless search runs counter to section 8 of the *Canadian Charter of Rights and Freedoms*. Even where a search has been authorized, the authorization may be challenged under the *Charter*. Two criteria have been developed in this regard. First, the person who authorizes the search, whether or not that person is a judge, must be in a position to appreciate in an entirely neutral and impartial manner the rights of the parties in question – the state and the individual. Second, the person who wishes to obtain such authorization must give evidence under oath of the existence of reasonable grounds (and not mere suspicions) for believing that an offence has been committed and that evidence is to be found in the place where the search is to be carried out.