Legislative Summary **LS-519E**

BILL C-74: MODERNIZATION OF INVESTIGATIVE TECHNIQUES ACT

Dominique Valiquet
Law and Government Division

21 December 2005

Library of Parliament

Bibliothèque du Parlement

Parliamentary Information and Research Service

LEGISLATIVE HISTORY OF BILL C-74

HOUSE OF COMMONS		SENATE	
Bill Stage	**Date**	**Bill Stage**	**Date**
First Reading:	15 November 2005	First Reading:	
Second Reading:		Second Reading:	
Committee Report:		Committee Report:	
Report Stage:		Report Stage:	
Third Reading:		Third Reading:	

Royal Assent:

Statutes of Canada

N.B. Any substantive changes in this Legislative Summary which have been made since the preceding issue are indicated in **bold print**.

Legislative history by Peter Niemczak

CE DOCUMENT EST AUSSI PUBLIÉ EN FRANÇAIS

TABLE OF CONTENTS

Page

Page

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

BILL C-74: MODERNIZATION OF INVESTIGATIVE TECHNIQUES ACT*

BACKGROUND

A. Lawful Access

Bill C-74 was introduced in the House of Commons by the Minister of Public Safety and Emergency Preparedness (the Minister) on 15 November 2005. It deals with very specific aspects of the rules governing lawful access, which is an investigative technique used by law enforcement agencies and national security agencies.(1) It involves intercepting communications(2) and seizing information(3) where authorized by law.

B. Purposes of the Bill

The bill creates the Modernization of Investigative Techniques Act (MITA), which has two objectives: first, to compel telecommunications service providers to have the capability to intercept communications made using their networks; and second, to provide law enforcement agencies with access to certain basic information identifying telecommunications service subscribers, on request.

---

* Notice: For clarity of exposition, the legislative proposals set out in the bill described in this legislative summary are stated as if they had already been adopted or were in force. It is important to note, however, that bills may be amended during their consideration by the House of Commons and Senate, and have no force or effect unless and until they are passed by both Houses of Parliament, receive Royal Assent, and come into force.

(1) In the interests of conciseness, references in this text to "law enforcement agencies" include national security agencies, unless otherwise clearly indicated by the context.

(2) This technique, commonly called "wiretapping," is very useful for investigating a variety of crimes, in particular drug-related offences. For the precise number of convictions secured through the use of wiretaps, among other techniques, see Public Safety and Emergency Preparedness Canada, *Annual Report on the use of Electronic Surveillance – 2004*, Figures 3 and 4, http://www.psepc-sppcc.gc.ca/abt/dpr/le/elecsur-en.asp.

(3) During a search.

It is essential to note, at the outset, that private communications may still be intercepted only with judicial authorization.(4) The bill makes no change to that requirement. The first objective relates solely to the *technical capability* of the transmission apparatus to intercept communications. Law enforcement agencies will thus be able to intercept both communications carried by traditional telephone networks and communications that use new technologies such as the Internet. However, the interception of an Internet communication, like a telephone communication, will also require that an application be made to a judge.

The second objective of the bill relates only to certain *identifiers associated with the subscriber*, such as the subscriber's name and address. Accordingly, the special system established for providing this kind of information does not include Web sites visited or the content of electronic mail. To obtain that information, law enforcement agencies must obtain a warrant or other judicial authorization, as they must for any information other than the identifiers specified in the bill and the regulations.

While the bill provides definitions for certain expressions and outlines the new rules, the regulations that are to be made will provide the necessary details and establish technical standards.

C. Basis of the Bill

1. Consultations

Since 1995, the Canadian Association of Chiefs of Police (CACP) has been calling for legislation to compel all telecommunications service providers to ensure that they have the capability to enable police services to carry out interceptions on their networks.(5) While the reform initiative began in the 1990s – that is, before the attacks of 11 September 2001 – the Department of Public Safety and Emergency Preparedness argues that the bill is necessary in order to combat terrorism more effectively.(6) The Department also cites the fight against organized crime.

---

(4) It should be noted, however, that judicial authorization is not necessary if the interception is carried out by the Communications Security Establishment (CSE) under Part V.1 of the *National Defence Act*, R.S. 1985, c. N-5. On the other hand, provision is made for other protection measures.

(5) Public Safety and Emergency Preparedness Canada, *Modernization of Investigative Techniques Act – Chronology*, 15 November 2005, http://www.sgc.gc.ca/media/bk/2005/bk20051115-1-en.asp.

(6) Technical information session held by Public Safety and Emergency Preparedness Canada, 15 November 2005.

After a strategic framework was developed, in 2000, representatives of Justice Canada, Industry Canada and the Solicitor General of Canada held public consultations, from August to December 2002. Over 300 submissions were received, from police services, industry, civil rights groups and individuals. A summary of the results of the consultations was released in 2003. This was followed by a series of meetings with stakeholders in 2005.

2. New Technologies

Canadians have access to an ever-growing number of new communications technologies. More than half of all households have a cell phone and Internet access at home.(7)

According to law enforcement agencies, new technologies such as wireless data networks and voice over Internet protocol(8) often present obstacles to the lawful interception of communications.(9) Such technologies can create "intercept safe havens" where criminal groups are able to operate without being detected. In light of factors such as deregulation of the telecommunications market, the growing complexity of telephone networks makes investigators' work more difficult and results in delays in identifying suspects.

Bill C-74 therefore requires that telecommunications service providers have interception capability, regardless of what technology they use. It covers all types of technology, both existing and future.

3. International(10)

Some countries, including the United States, the United Kingdom, France, Germany, Australia, New Zealand and South Africa, have enacted legislation regarding the interception of communications transmitted using new technologies.

On 23 November 2001, Canada signed the Council of Europe's *Convention on Cybercrime*. The Convention makes it an offence to commit certain crimes using computer

---

(7) Moreover, "Canadians send more than 2.7 million text messages a day" (Office of the Privacy Commissioner of Canada, *Response to the Government of Canada's "Lawful Access" Consultations*, 5 May 2005, http://www.privcom.gc.ca/information/pub/sub_la_050505_e.asp).

(8) Voice over IP (VoIP). There are also new and more effective service options, and new calling characteristics; satellite communication; beepers and personal digital assistants (PDAs) that use protected algorithms; and high-speed data transmission overlay networks that allow for the wireless transmission of data packets.

(9) Nevis Consulting Group Inc., ed., *Summary of Submissions to the Lawful Access Consultation*, 28 April 2003, pp. 5, 18 and 36-37. Among other things, the inability to crack encryption and a lack of common data-sharing protocols are said to cause problems.

(10) This aspect will be analyzed in greater detail in a separate publication.

systems[11] and creates legal tools to make it possible to investigate criminal activities that use new technologies.[12] Because international cooperation is essential to address an area in which crime knows no borders, the treaty also aims to facilitate information-sharing among different countries' law enforcement agencies.

Bill C-74 is thus a means of equipping Canada with legislation similar to that of other countries and implementing certain measures of the *Convention on Cybercrime*.[13]

D. Measures Not Included in the Bill

A number of measures proposed in the consultations were not incorporated in the bill. Strong opposition to the creation of a national database and the imposition of storage and "know your customers" obligations will doubtless continue, particularly on the part of privacy advocates. It is possible, however, that certain measures such as preservation and production orders may be the subject of subsequent bills.

1. Storage Obligation and National Database

The bill does not require telecommunications service providers to collect and preserve information about their subscribers. Service providers will therefore not be obliged to systematically collect and preserve information on Canadians' Internet surfing activities.

As well, a national database containing information about telecommunications service subscribers, including both identifying information (e.g., names and addresses) and communications activities, will not be established.

2. "Know Your Customers"

The bill does not impose an obligation on telecommunications service providers to ascertain the identity of their subscribers.[14] Anonymous services, such as prepaid phone cards, will therefore still be legal.

---

(11) Including Internet fraud, child pornography and offences relating to computer viruses. An additional protocol addresses hate propaganda.

(12) These include preservation and production orders (including an order for the production of "subscriber information").

(13) In order for Canada to ratify the Convention, it would have to amend the *Criminal Code*, *inter alia* to include preservation and production orders and to expand the offence relating to computer viruses.

(14) This measure is not included even though law enforcement agencies believe that prepaid cell phone services, Internet access cards, Internet cafes and Internet facilities in public libraries complicate investigators' jobs (Nevis Consulting Group Inc. (2003), p. 18).

3. Preservation Order

This is a judicial order, made on reasonable grounds, that is in effect for the time needed by the law enforcement agency to obtain a search warrant or production order. It is therefore an expedited measure for protecting information that might easily be destroyed or modified in the intervening time.

A preservation order requires the service provider to preserve information regarding a particular transaction or a person whose communications are authorized to be intercepted. Preservation must relate to an investigation and to information that has already been stored.(15)

The federal institutions responsible for the consultations also proposed that when a law enforcement agency is facing an urgent situation, it should be able to require a service provider to preserve information without first obtaining authorization from a judge.(16) That measure would be valid for only a short time, however.

While Bill C-74 does not contain such a measure, a preservation order may be introduced in the form of an amendment to the *Criminal Code* (the Code).(17)

4. Specific Production Order

This type of judicial order, which also requires that there be reasonable grounds before it is issued, is similar to a search warrant. However, instead of the law enforcement agency going on site to obtain the information sought, the telecommunications service provider produces the information requested. Law enforcement agencies can thus obtain documents that are located in another country.

The Code provides for a procedure for obtaining a general production order, that is, an order that applies regardless of the type of information a law enforcement agency is seeking.(18) Issuance of such an order is based on the existence of reasonable grounds for *believing* that an offence has been committed (stringent test).(19) A specific production order is also available to obtain a record of telephone calls.(20) Issuance of this kind of order is based on

(15) A preservation order does not require a service provider to collect and store certain data relating to all of its subscribers.

(16) Department of Justice, Industry Canada and Solicitor General of Canada, *Lawful Access – Consultation*, 25 August 2002, p. 14.

(17) R.S. 1985, c. C-46.

(18) Section 487.012 of the Code. There is also provision for such an order in the *Competition Act*, R.S. 1985, c. C-34 (para. 11(1)(*b*)).

(19) Paragraph 487.012(3)(*a*) of the Code.

(20) Subsection 492.2(2) of the Code.

the existence of reasonable grounds for *suspecting* that an offence has been or will be committed (less stringent test).(21)

A proposal was put forward during the 2002 consultations to create a production order to obtain information from service providers showing telecommunications traffic data.(22) Like an order relating to records of telephone calls, the proposed production order could have been made on the basis of the less stringent test: the presence of reasonable grounds for suspecting.(23) Bill C-74 does not contain an order of this nature.

5. Electronic Mail

The bill does not resolve the debate regarding how electronic mail should be treated. It does not specify which rules will apply to electronic mail: Part VI of the Code(24) or the provisions relating to search warrants.(25)

The Part VI rules are more stringent than those relating to search warrants.(26)

---

(21) *Ibid*. The Code also uses the test of reasonable grounds for suspecting in the case of an order to produce banking information (subsections 487.013(1) and (4)) and in the case of a warrant to install a tracking device (subsections 492.1(1)).

(22) This is essentially information showing the origin, destination, date, time, duration and volume of a telecommunication.

(23) Because traffic data do not disclose the content of the communication, collection of these data is regarded as a less significant invasion of privacy. This was the position, at least, of the federal institutions responsible for the 2002 consultations (*Lawful Access – Consultation* (2002), p. 12). See also Council of Europe, *Convention on Cybercrime – Explanatory Report*, http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

(24) Sections 183 *et seq.* of the Code.

(25) The rules governing searches and seizures are set out in, *inter alia*, ss. 487 *et seq.* of the Code and ss. 15 and 16 of the *Competition Act*. The same kind of questions can also be asked regarding on-line chat and instant messaging. In addition, there is a question as to whether different rules should apply, depending on where the electronic message is located. For example, on the one hand, a police service would need to obtain a search warrant to seize electronic mail in transit from the originator's or intended recipient's Internet provider. On the other, it would have to abide by the rules in Part VI concerning the interception of electronic mail in the originator's or intended recipient's inbox.

(26) Part VI of the Code contains additional protection measures. In order for a judge to authorize the interception of a private communication, the judge must be satisfied that, *inter alia*, the interception would be in the best interests of the administration of justice [para. 186(1)(*a*) of the Code) and there is no other reasonable investigative procedure in the circumstances (para. 186(1)(*b*) of the Code. This is the necessity requirement. On this point, see the Supreme Court decision in *R.* v. *Araujo*, [2000] 2 S.C.R. 992. It should be noted, however, that the necessity requirement does not apply when the interception relates to a terrorism offence or organized crime (subsection 186(1.1) of the Code)). In addition, only certain specified offences can justify interception by a police service (the list of offences is found in s. 183 of the Code. Interception of communications with the consent of the originator or recipient ("participatory" or "consensual" surveillance), however, applies to any offence set out in the Code or any other Act of Parliament (para. 184.2(2)(*a*))].

Part VI allows police services to intercept a "private communication."[27] If an e-mail is indeed a telecommunication, it is not certain that the originator may reasonably expect that only the intended recipient will read it.[28] Messages of this kind can be easily intercepted.[29] On the other hand, why make a distinction between an e-mail and a fax or a telephone call, particularly when electronic mail may contain information and sensitive personal data?

DESCRIPTION AND ANALYSIS

Rules relating to lawful access are set out in a number of federal statutes, in particular the *Criminal Code*, the *Canadian Security Intelligence Service Act*[30] and the *National Defence Act*.[31] Clause 2(2) of Bill C-74 provides, for greater certainty, that law enforcement agencies retain the powers conferred by those Acts.[32] Bill C-74 enables law enforcement agencies to exercise those powers regardless of the technology used by telecommunications service providers (interception capability). It also provides for certain agencies to have access to basic information relating to telecommunications service subscribers (subscriber information). In addition to discussing those two key aspects of the bill, this paper will address the question of penalties and exemptions. It will not however, examine each of the bill's 59 clauses in detail.

---

(27) Section 183 of the Code defines "private communication" as follows: "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it." Section 35 of the *Interpretation Act*, R.S. 1985, c. I-21, provides the following definition of telecommunications: "the emission, transmission or reception of signs, signals, writing, images, sounds or intelligence of any nature by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system."

(28) Robert W. Hubbard, Peter M. Brauti, and Scott K. Fenton, *Wiretapping and Other Electronic Surveillance*, Canada Law Book, No. 11, Aurora, September 2005, pp. 1-10.1 and 6-22.4.

(29) See *R. v. Weir*, [1998] 8 W.W.R. 228 (Alta. Q.B.).

(30) R.S. 1985, c. C-23.

(31) As noted earlier, the *Competition Act* also contains provisions relating to searches, seizures and production orders.

(32) See also clause 21 of the bill.

A. Interception Capability

1. Present Situation

At present, there is no Canadian legislation compelling all telecommunications service providers to use apparatus that is capable of intercepting communications. Only licensees that use radio frequencies for wireless voice telephone services(33) have been required, since 1996, to have facilities that permit such interceptions.(34) There is no similar legislation for other telecommunications service providers.

2. Situation Under the Bill

Bill C-74 is designed to remedy this absence of standards for the interception capability of telecommunications service providers. It requires all service providers – for example, Internet service providers (ISPs) – to possess apparatus(35) that enables law enforcement agencies to intercept communications sent to a service provider, after a judicial authorization has been obtained. The bill therefore applies, subject to specified exemptions, to all telecommunications service providers that operate a transmission facility in Canada.(36)

Moreover, the requirement for uniform interception capability relates both to transmission data and to the actual content of the communication (clauses 2,(37) 6 and 7). An ISP must therefore use apparatus that enables law enforcement agencies to identify, for example, on the one hand, subscribers' e-mail and Internet protocol (IP) addresses,(38) the date and time of communications and the type of file transmitted (transmission data) and, on the other hand, the Web pages visited and the substance of messages (content-related data).

---

(33) Referred to as "personal communications services" (PCS), which essentially means wireless digital telephones.

(34) This requirement is imposed by Industry Canada when issuing spectrum licences under the *Broadcasting Act* (S.C. 1991, c. 11). The rules governing interception are set out in the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications* (revised in November 1995). See Kirsten Embree, "Lawful Access: A Summary of the Federal Government's Recent Proposals – Part I," *Internet and E-Commerce Law in Canada*, Vol. 6, May 2005, p. 18, and the Industry Canada Web site, *Spectrum Management and Telecommunications – Personal Communications Services*, http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/en/h_sf02092e.html.

(35) Technical standards will be set out in the regulations.

(36) A number of telecommunications service providers in Canada, however, have only an administrative office in this country, their telecommunications facilities being in the United States.

(37) Defining the expressions "communication" and "transmission data."

(38) The address may be static or change each time a connection is made (dynamic IP).

3. Entry Into Force of the Obligations

Bill C-74 does not require telecommunications service providers to meet the technical standards for interception capability immediately. Rather, it requires them to maintain their existing interception capability (clause 8), even when they provide new services (clause 9).

On the other hand, service providers must comply with the new technical interception standards when they update their systems – that is, when they acquire new transmission apparatus (clause 10) or install new software (clause 11). Even in those cases, the bill provides for a 12-month transition period (clause 58). Thus a service provider that, for example, installs new software after the bill comes into force will not have to comply with the technical standards until the first anniversary date of the legislation. A new telecommunications company that enters the market after that date will have to meet the technical interception capability requirements (clause 10).

However, the Minister has the power to issue a ministerial order requiring a telecommunications service provider to acquire communications interception capability that meets the technical standards before upgrading (clause 15(1)(*d*) and (*e*)). It should also be noted that the Minister must pay compensation in an amount that the Minister considers reasonable to cover the expenses incurred to comply with an order, regardless of the purpose of that order (clause 15(3)).

4. Obligations

a. Comply with Requests and Provide Information

Once a law enforcement agency has obtained a judicial authorization, the telecommunications service provider must comply with any request relating to the interception of communications (clause 6(1)). Under the regulations policy adopted by the Department of Public Safety and Emergency Preparedness, a telecommunications service provider must allow law enforcement agencies to intercept communications as soon as possible after receipt of a written or oral notice, and at the latest within:

- two business days;
- 30 minutes to eight hours in exceptional circumstances.[39]

(39) For example, in an urgent situation in which national security is jeopardized.

The service provider must provide the intercepted communication in the form specified by regulation (clause 6(1)(*a*) and (3)). As well, the service provider is required to provide law enforcement agencies, on request, with information relating to its facilities and the telecommunications services it offers to subscribers in general or to a person whose communications are the subject of a court order authorizing their interception (clauses 6(1)(*c*) and 23).

b. Provide Assistance

A telecommunications service provider has a legal obligation to provide assistance to any law enforcement agency to permit it to assess telecommunications facilities (clause 24).[40] For example, it may confirm that the devices actually intercept communications and that the latter are in fact the communications of the person who is the subject of the court order.

The service provider must prepare a list of the names of the employees who may provide assistance. The list must be available, on request, to law enforcement agencies, which may conduct an investigation for the purposes of a security assessment of any of the persons on the list (clause 27).

c. Confidentiality

All interception processes must be kept confidential (clause 6(1)(*d*)).[41] Telecommunications service providers are thus required to comply with the regulations and to guarantee the security of the contents of the intercepted communication, the traffic data and the identity of the individuals and organizations involved.

(40) Assistance orders are found in, *inter alia*, s. 487.02 of the Code. Such an order applies to all actions taken under an interception authorization or search warrant.

(41) However, a police service that has carried out an interception under Part VI of the Code has an obligation to inform the person who was the subject of the interception in writing. The usual 90-day period (subsection 196(1)) has been extended to three years in the case of organized crime and terrorism offences (subsection 196(5)). That obligation does not apply to interceptions carried out by the Canadian Security Intelligence Service or the Communications Security Establishment.

d. Real-time Interception

Clause 7(*a*) provides, generally, that telecommunications service providers must have the capability to intercept communications in accordance with the technical standards to be established in the regulations made under the proposed Act.

Real-time collection of transmission data is an important investigative technique that can be used, *inter alia*, to identify the source of the intrusion or broadcast. Under the regulations policy, if a service provider does not have the capability to intercept such data in real time, it must at least be capable of intercepting them one second after interception of the content of the communication.

e. Isolate the Communication

A judicial authorization to intercept communications will be made for one or more specific individuals. The telecommunications service provider must therefore be able to separate the communications of the person for whom the authorization is granted from the communications of other users (clause 7(*b*)(i)). It must also have the capability to isolate the transmission data from the data relating to the contents of the communication (clause 7(*b*)(ii)).

f. Correlation

A telecommunications service provider must also have the technical capability to do exactly the opposite of what was described above: link traffic data to the content of an intercepted communication (clause 7(*c*)). The law enforcement agency will then be able to associate the offence committed and an IP address, for example.

g. Simultaneous Interceptions

Telecommunications service providers are required to allow law enforcement agencies to intercept communications transmitted at the same time by more than one user (clause 7(*d*)). The regulations will establish the minimum and maximum[42] numbers of simultaneous interceptions that telecommunications facilities will have to support (clauses 7(*d*)(ii) and 13). The Minister may, however, order a service provider to take measures to increase the number of simultaneous interceptions to a number greater than the maximum (clause 15(1)(*b*)).

---

(42) The regulations policy provides for a minimum of two simultaneous interceptions, while the maximum depends on the number of subscribers.

h. Encryption

At present, wireless digital communications service providers have an obligation, under their operating licence conditions, to provide law enforcement agencies with decrypted communications. The bill extends that obligation to all technologies (clause 6(1)(*b*)). If measures taken to protect a communication, such as encrypting or encoding, have been applied by someone other than the service provider and the service provider is unable to remove them, it must then provide all reasonable assistance to law enforcement agencies to do so (clauses 6(1)(*b*)(ii) and 6(2)).(43)

5. Reporting

All telecommunications service providers must submit a report to the Minister stating their capability to respond to the interception requirements set out in the bill (clause 28).(44) They must submit that report within six months of the date on which the bill comes into force, when transmission apparatus is acquired, and at any time that the Minister so requires.

B. Subscriber Information

1. Present Situation

At present, law enforcement agencies must have a warrant or court order in order to compel telecommunications service providers to provide them with personal information about their clients that is in their possession.(45)

2. Situation Under the Bill

The bill establishes a set of special rules that enable certain designated people to compel a telecommunications service provider, without a warrant or court order, to provide them

---

(43) At the international level, see the Wassenaar Arrangement (concluded in 1996) which relates to, *inter alia*, control of dual-use technologies (http://www.wassenaar.org/).

(44) Those which meet all of the statutory requirements may, alternatively, provide a written statement to that effect.

(45) See para. 7(3)(*c*.1) of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c. 5. With respect to the protection of personal information, held by a company, that does not reveal intimate details of clients' lifestyle and personal choices, see *R. v. Plant*, [1993] 3 S.C.R. 281 (decision considered in a more recent decision of the Supreme Court: *R. v. Tessling*, [2004] 3 S.C.R. 432).

with basic information concerning one of their subscribers. The bill provides for protection measures in relation to such information requests.

3. Request for Information

a. Types of Information That May be Requested

The information covered by the special rules is strictly limited. The Department of Public Safety and Emergency Preparedness likens it to the information that can be found in a telephone directory.

The information in question consists solely of basic identifying information about a subscriber, such as name, IP address, e-mail address, telephone number, cell phone number, or any unique number associated with such a device[46] (clause 17(1)). That information is often essential to law enforcement agencies in the performance of their duties, and in particular in conducting investigations. It may be used to obtain a warrant or other judicial authorization.

A distinction must be made between an account holder (the subscriber) and the actual user of the telecommunications, who may be two separate individuals. For example, the person who uses a computer terminal to commit an offence is not necessarily the person named on the Internet service invoices. Because of that uncertainty, and the possibility of an unjustified violation of privacy, the Federal Court has refused to order disclosure of the names of people whose Internet accounts were used to download copyrighted music files.[47] Under the bill, telecommunications service providers are required to provide such subscriber-related information on request by designated persons.

However, service providers are not required to collect information other than the information they already collect in the normal course of business. The bill uses the expression “any information in the service provider’s possession or control” (clause 17(1)). As well, they are not required to verify the accuracy of the information they collect.

b. Designated Persons

Only a designated person may make a request for information under the bill (clause 17(1)). The person is designated by the Commissioner of the Royal Canadian Mounted

(46) For example, an “electronic serial number” that is specific to a particular wireless device.

(47) *BMG Canada Inc.* v. *John Doe*, [2004] 3 F.C.R. 241, aff’d (2005) 334 N.R. 268 (F.C.A).

Police (RCMP), the Director of the Canadian Security Intelligence Service (CSIS), the Commissioner of Competition or a chief of police (clause 17(3)).

They may designate only a small number of employees in their organizations. The number of designated persons is limited to 5% of the agency's employees, or, where an organization has 100 or fewer employees, 5 persons (clause 17(4)).

c. A Police Officer, in an Urgent Situation

In an urgent situation that it is reasonably believed may result in serious harm to any person or to property, any police officer – instead of the designated persons – may make a request for information (clause 18(1)).[48] The police officer must, however, inform one of the designated persons in his or her organization, and that person will confirm the request to the telecommunications service provider in writing (clause 18(3)).

d. Investigation

A request for information may be made only in the course of an investigation by CSIS, the Competition Bureau or a police service, under the applicable legislation (clause 17(2)). The information obtained must be used solely for that purpose or for related purposes[49] (clause 19).

Because requests must relate to specific individuals, the designated persons are required to provide at least one identifier associated with the subscriber when the request is made, to avoid "fishing expeditions."[50]

e. Reply

Under the regulations policy, the telecommunications service provider must provide the information as soon as possible after receiving the request, and at the latest:

- within two business days (written reply);
- within 30 minutes in an emergency situation (written or oral reply).

(48) The same exceptional circumstances as those set out in s. 184.4 of the Code, relating to the interception of communications.

(49) Law enforcement agencies may, for example, use the information obtained to lay criminal charges.

(50) For example, to obtain a subscriber's name, a designated person could provide an IP address. See the regulations policy with respect to other possible situations.

f. Confidentiality

The entire process surrounding the request for information is kept confidential. The telecommunications service provider must not inform a subscriber that a designated person has made a request or that it has provided information to the designated person (clause 22).

4. Protection Measures

The provisions relating to information about subscribers are an attempt to strike a balance between expanding the powers of law enforcement agencies and protecting individuals' privacy. While law enforcement agencies are able to obtain this information without a warrant, the bill does establish certain extrajudicial protection measures.

a. Records

It must be possible to trace every request for information. The request must therefore be made in writing (clause 17(1)). Designated persons are also required to keep a record that contains, *inter alia*, the reasons for each request and the information obtained (clause 17(6)).

b. Internal Audits

The Commissioner of the RCMP, the Director of CSIS, the Commissioner of Competition or a chief of police are required to take measures to verify, on a regular basis, that the requests made by their organization comply with the MITA (clause 20(1)). Among other things, the records and the use made of the information must therefore be examined.

Reports must be submitted concerning the results of the audits. A report must be made each time the Commissioner of the RCMP, the Director of CSIS, the Commissioner of Competition or a chief of police deems it necessary (clause 20(2)). The report must be provided to:

- the Minister and the Privacy Commissioner, if it concerns the RCMP;
- the Minister and the Security Intelligence Review Committee, if it concerns CSIS;
- the Minister of Industry and the Privacy Commissioner, if it concerns the Commissioner of Competition;

- the attorney general of the province and the provincial privacy commissioner, if it concerns a chief of police (clause 20(2), (3) and (7)).

c. External Audits

The Privacy Commissioner (and the provincial privacy commissioners, under their respective powers, for police services in the provinces) has the power to conduct audits to determine whether the RCMP or the Commissioner of Competition is in compliance with the provisions relating to requests for information (clause 20(4)). The Security Intelligence Review Committee may also undertake external audits in respect of CSIS (clause 20(5)).

C. Penalties

The bill provides for two types of contraventions of the MITA: violations or offences. It establishes what is essentially a code of penal procedure for violations, which are apparently less serious contraventions. For offences, the summary conviction procedure set out in the Code applies.[51] In both instances, however, charges must be laid within two years of the date on which the subject matter of the proceedings arose (clauses 45 and 56), and the accused may argue that he or she exercised due diligence as a defence to a charge of contravening the law (clauses 43 and 53).

In addition, the Minister may appoint inspectors and enforcement officers who will monitor telecommunications service providers' compliance with the MITA (clauses 32(1) and 35(1)). They have the power to enter any place owned by a telecommunications service provider to examine any document and telecommunications facilities (clauses 33(1) and 35(3)).

Finally, it should be noted that, in respect of the obligations relating to information about subscribers, the bill says nothing about the applicable penalty.

1. Offences

The bill subdivides offences into three categories, based on the amount of the fine that may be imposed. It must be emphasized that no offence (and *a fortiori* no violation) is liable to imprisonment.

---

(51) Part XXVII of the Code.

A breach of the obligations relating to capability to intercept, or contravention of a ministerial order, is liable to maximum fines: $100,000 in the case of an individual and $500,000 in the case of a corporation (clause 51). In addition, if a telecommunications service provider does not have the required capability to intercept when its system is updated, a court may issue an injunction to prevent the use of transmission apparatus or software (clause 57).

Every person who makes a change to a law enforcement agency's interception equipment, fails to submit a report concerning interception capability, makes a false statement or fails to comply with the conditions of an exemption is liable to a fine not exceeding $25,000 in the case of an individual ($50,000 for a subsequent offence) or $100,000 in the case of a corporation ($250,000 for a subsequent offence) (clause 52(1)).

Failing to cooperate or obstructing the work of an inspector constitutes an offence punishable by a fine not exceeding $15,000 (clause 52(2)).

2. Violations

The Governor in Council, on the recommendation of the Minister, will determine, by regulation, which contraventions of the MITA or the regulations will constitute a violation (clauses 31(1)(*g*)(i) and 34). The regulations will also establish the maximum fine that may be imposed for a particular violation. The amount of the fine may not exceed $50,000 in the case of an individual and $250,000 in the case of a corporation (clauses 31(1)(*g*)(ii) and 34).

The bill lays down the outline for the procedural rules:

- If there are reasonable grounds to believe that a violation has been committed, an enforcement officer will issue a notice of violation on the person believed to have committed it (clause 36(1)).

- The notice of violation will state the fine that the enforcement officer proposes to impose, taking into account the factors set out in the MITA and the regulations (clause 31(1)(*g*)(iii), clause 36(2)(*c*) and clause 36(3)). The person believed to have committed the violation then has three choices:
  i. Pay the fine. This terminates the proceedings (clause 37).
  ii. Contest the facts alleged or the amount of the fine, by making representations to an enforcement officer other than the one who issued the notice of violation, within 30 days or within any longer period specified in the notice (clauses 36(2)(*d*) and 38(1)). That enforcement officer will decide on a balance of probabilities (clause 38(2)). The maximum fine that the enforcement officer may impose is the amount stated in the notice of violation. An appeal to the Minister is then available (clauses 31(1)(*g*)(vi) and 40).

iii. Neither pay the fine nor make representations. This amounts to an admission of liability and the person must then pay the fine specified in the notice of violation (clauses 36(2)(*e*) and 39).

D. Exemptions

1. Complete Exemption

a. "Private Networks"

The bill, in its entirety, does not apply to "private networks" (clause 5(1)). This means persons who provide telecommunications services primarily to themselves, their household or their employees, and not to the public.

b. Specified Institutions

As well, no provision of the bill applies in the case of:

- registered charities;
- educational institutions (except post-secondary institutions);
- hospitals;
- places of worship;
- retirement homes;
- telecommunications research companies;(52)
- broadcasting undertakings(53) (only in respect of broadcasting (clause 5(1)).

2. Partial Exemption

a. "Intermediaries"

Telecommunications service providers that act as "intermediaries," that is, that transmit communications on behalf of other telecommunications service providers but do not modify communications or authenticate the users, are not subject to the obligations in respect of interception capability when they upgrade their systems or to the obligations in respect of

(52) For example, CANARIE (http://www.canarie.ca/).

(53) Within the meaning of subsection 2(1) of the *Broadcasting Act*.

subscriber information (clause 5(2)). However, they may be made subject to these by order of the Minister.

b. Specified institutions

Apart from the obligation to provide information to law enforcement agencies regarding their telecommunications facilities and services, the bill does not apply to telecommunications service providers whose principle operation is:

- a post-secondary educational institution;
- a library;
- a community centre;
- a restaurant;
- a hotel or apartment building (clause 5(3)).

c. Exemption Order

The Governor in Council may, on the recommendation of the Minister and the Minister of Industry, make an order exempting certain categories of telecommunications service providers from the most significant obligations in the bill, including obligations relating to interception capability when systems are upgraded or obligations relating to subscriber information (clause 30(1)). The order may impose conditions, and the exemption granted may not be valid for more than two years (clause 30(3)).

d. Order Suspending Obligations

The Minister may, by order made on the application of a telecommunications service provider stating reasons, suspend in whole or in part any obligation relating to interception capability, when systems are upgraded (clause 14(1), (2) and (5)). The Minister may include any conditions that he or she considers appropriate (clause 14(5)).

e. “Small Telecommunications Service Providers”

The bill grants a three-year exemption for service providers with fewer than 100,000 subscribers (clause 12). During that period, a small service provider does not have to comply with the interception capability standards that must be met when it upgrades its system.

However, it must provide a physical connection point permitting law enforcement agencies to intercept communications.

E. Coming Into Force

The bill will come into force by order of the Governor in Council on one or more dates. In the latter case, different provisions of the bill would come into force at different times (clause 59).

COMMENTARY[54]

A. Law Enforcement Agencies

During the consultations, law enforcement agencies generally supported the lawful access proposals. They were of the view that there must not be "safe havens" in Canada where it is impossible to intercept communications, and that a service provider that failed to meet the obligation to guarantee interception capability should be liable to a large fine. As well, a request for the suspension of obligations relating to interception capability should not be granted if it is made five years after the Act comes into force.

With respect to subscribers' names and addresses, law enforcement agencies do not regard these as personal information. They agreed that they should be able to have access to them without a warrant or court order. On the other hand, a national database should also have been created, that would contain this kind of information.

B. Industry

While the industry generally supports the idea of permitting effective lawful access in the face of technological change, some doubt was expressed as to the need for the bill. It was suggested that there is no evidence that any investigations had failed because of inadequate technical interception capability.

The question of the costs associated with implementing a standard interception capability is of particular concern to telecommunications companies.[55] They also argue that

---

(54) Most of the information that follows is taken from Nevis Consulting Group Inc. (2003). Many of the arguments are still being made today.

(55) For example, the costs associated with "usage rights" for software that allows for certain specific functions to be activated.

providing lawful access services to law enforcement agencies, such as providing subscriber information and assisting them in interception procedures, generates high ongoing costs in terms of personnel, training and security.(56) If the government does not offer reasonable compensation, those costs will have to be borne by consumers. A group composed of telecommunications companies and representatives of police services has suggested that the money confiscated from criminals be used to fund the new lawful access measures.(57)

Telecommunications companies oppose the establishment of technical interception requirements that are unique to the Canadian market.(58) Given the differences in the size of the markets, Canadian companies would have to bear higher costs. Some associations(59) have therefore proposed that companies not be held to the Canadian requirements until the necessary apparatus is available at reasonable cost. They also argue that compliance with international standards would allow the obligations set out in the Canadian regulations to be met. The Canadian industry should also be able to participate in developing the technical standards.

In addition, the question of costs and technical standards should be dealt with by legislation rather than by regulations, as a full parliamentary review should be undertaken.

With regard to subscriber information, it was pointed out that cybercriminals can always use false names, pirated accounts or computers to which the public has access.

C. Privacy and Information Commissioners

(56) Campbell Clark, "Ottawa demands greater wiretap access," *The Globe and Mail* [Toronto], 11 October 2005, p. A1.

(57) Jim Bronskill, "New proposal would have criminals foot wiretap bill: Controversial law could be introduced next month," *Montreal Gazette*, 31 October 2005, p. A11.

(58) The proposed technical requirements relating to interception capability would go farther than those imposed in other countries. They would encompass services not covered by the American rules (ANSI) or European rules (ETSI) (Kirsten Embree, "Lawful Access: A Summary of the Federal Government's Recent Proposals – Part II," *Internet and E-Commerce Law in Canada*, Vol. 6, June 2005, p. 34; see also Tyler Hamilton, "Telecoms feel heat on wiretaps," *Toronto Star*, 22 February 2005, p. D01).

(59) The Canadian Wireless Telecommunications Association (CWTA), the Canadian Cable Telecommunications Association (CCTA) and the Information Technology Association of Canada (ITAC).

Privacy advocates also expressed doubts as to the need for new lawful access rules.(60) They argue that it has not been demonstrated that existing legislation is insufficient.

Law enforcement agencies can already intercept communications transmitted using new technologies. For example, keyboard recorders can record e-mails and obtain passwords, packet sniffers can sweep messages to detect specific words, and cell phones are equipped with systems that can be used to track an individual.(61) The obligations relating to interception capability open the door even wider to abuse by law enforcement agencies.(62)

If service providers are compelled to have interception capability, and to some extent to play a role in surveillance of communications, the boundary between the private and public sectors will be eroded, making telecommunications service providers agents of the state. In addition, intercepting an Internet communication can reveal a lot more personal information than wiretapping a telephone conversation, and therefore calls for a different approach to be taken. Moreover, the new measures regarding lawful access may engender public distrust of the new technologies by reinforcing the belief in constant surveillance by "Big Brother."

When someone's name or address is combined with a unique identifier such as a telephone number, the rules that protect privacy should come into play. Existing legislation that offers that protection should not be amended in order to gain access to this kind of information without a warrant.

D. Civil Society Groups(63)

Civil society groups felt that the consultation document was unconvincing on how the measures would actually help fight terrorism or organized crime. In that respect, it was pointed out that there were no statistics to support new lawful access legislation. As an alternative to the imposition of new obligations, law enforcement agencies should instead be

(60) Office of the Privacy Commissioner of Canada, *Response to the Government of Canada's "Lawful Access" Consultation* (2005).

(61) For example, global positioning systems (GPS).

(62) Clark (2005).

(63) "[C]ivil society groups comprise civil liberty associations, community groups, consumer representatives, non-governmental privacy/freedom of information organizations and associations representing the legal profession" (Nevis Consulting Group Inc. (2003), p. 3).

given the technical expertise and equipment they need to deal with changes in the nature of crime and in technology.

As well, given that the technical requirements for interception will apply only when systems are upgraded, this could amount to a disincentive to improve equipment and services. Some service providers will prefer not to update their systems so that they will not be compelled to meet the new standards.

The question of subscriber information is also problematic. Law enforcement agencies should still have to obtain a warrant or court order in order to get access to such information. The protection measures provided in the bill are not sufficient.(64)

E. General Public

Here again, the question was raised as to what urgent need the lawful access measures are responding to. The federal institutions responsible for the consultations failed to make the case for the problems that the Internet has created for law enforcement agencies.

The protection measures that apply to requests for subscriber information are insufficient, and measures should be implemented prior to information being disclosed, not just once the law enforcement agency has actually obtained the information requested.

There were also concerns that the new obligations would ultimately result in higher charges for users.

---

(64) Campbell Clark, “Privacy advocates blast Web surveillance bill,” *The Globe and Mail* [Toronto], 16 November 2005, p. A6.