Legislative Summary **LS-655E**

BILL C-47: TECHNICAL ASSISTANCE FOR LAW ENFORCEMENT IN THE 21ST CENTURY ACT

Dominique Valiquet
Legal and Legislative Affairs Division

28 July 2009

Library of Parliament
Bibliothèque du Parlement

Parliamentary Information and Research Service

LEGISLATIVE HISTORY OF BILL C-47

HOUSE OF COMMONS		SENATE	
Bill Stage	**Date**	**Bill Stage**	**Date**
First Reading:	18 June 2009	First Reading:	
Second Reading:	29 October 2009	Second Reading:	
Committee Report:		Committee Report:	
Report Stage:		Report Stage:	
Third Reading:		Third Reading:	

Royal Assent:

Statutes of Canada

This bill did not become law before the 2nd Session of the 40th Parliament ended on 30 December 2009.

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

CE DOCUMENT EST AUSSI PUBLIÉ EN FRANÇAIS

CONTENTS

Page

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

BILL C-47: TECHNICAL ASSISTANCE FOR LAW ENFORCEMENT IN THE 21ST CENTURY ACT*

BACKGROUND

A. Purpose of the Bill: Lawful Access

Bill C-47, An Act regulating telecommunications facilities to support investigations (short title: Technical Assistance for Law Enforcement in the 21st Century Act), was introduced in the House of Commons on 18 June 2009, by the Minister of Public Safety (the minister), the Honourable Peter Van Loan.

It deals with very specific aspects of the rules governing lawful access. Lawful access is an investigative technique used by law enforcement agencies(1) and national security agencies that involves intercepting communications(2) and seizing information where authorized by law. Rules relating to lawful access are set out in a number of federal statutes, in particular the *Criminal Code*, the *Canadian Security Intelligence Service Act* and the *National Defence Act*. For greater certainty, the bill provides that law enforcement agencies retain the powers conferred by those Acts.(3)

---

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

(1) In the interests of conciseness, the term "law enforcement agencies," when used in this text, includes national security agencies, unless otherwise clearly indicated by the context.

(2) Commonly called "wiretapping."

(3) Clause 2(2) of the bill.

This bill complements the current lawful access regime. It addresses the same two issues as the former Bill C-74:[4] technical interception capabilities of telecommunications service providers and requests for subscriber information.

Other aspects of the lawful access regime are addressed in Bill C-46, Investigative Powers for the 21st Century Act, which was introduced on the same day as Bill C-47.

B. Key Measures in the Bill

Bill C-47 addresses a concern expressed by law enforcement agencies, which contend that new technologies, particularly Internet communications, often present obstacles to lawful communications interception. The bill permits the following:

- It compels telecommunications service providers to have the capability to intercept communications made using their networks, regardless of the transmission technology used (clauses 6 to 15).
- It provides law enforcement agencies with access, under an accelerated administrative process without a warrant or court order, to basic information about telecommunications service subscribers. At the same time, the bill provides for certain protection measures (clauses 16 to 23).

C. Basis of the Bill

1. Consultations

Since 1995, the Canadian Association of Chiefs of Police (CACP) has been calling for legislation requiring that all telecommunications service providers have the technical means in place to enable police services to carry out lawful interceptions on their networks.

Following the development of a strategic framework in 2000, representatives of Justice Canada, Industry Canada and the Solicitor General of Canada held public consultations in 2002.[5] After having received more than 300 submissions from police services, industry, civil

---

(4) Bill C-74, An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information, 1st Session, 38th Parliament (died on the *Order Paper*). For more information about this bill, see Dominique Valiquet, *Telecommunications and Lawful Access: I. The Legislative Situation in Canada*, PRB 05-65E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 21 February 2006, http://lpintrabp.parl.gc.ca/LopImages2/prbpubs/bp1000/prb0565-e.asp.

(5) See Justice Canada, Industry Canada, and Solicitor General Canada, *Lawful Access – Consultation Document*, 25 August 2002, http://justice.gc.ca/eng/cons/la-al/consult.html.

rights groups and individuals, Justice Canada released a summary of the results of the consultations in 2003.(6) Throughout the consultations, protection of privacy was one of the central issues in the debate on lawful access. Other significant elements included technical interception standards, costs related to interception capability and the need for new lawful access rules.

The consultations led to the introduction, in November 2005, of Bill C-74, which would have created the Modernization of Investigative Techniques Act, but the bill died on the *Order Paper* before second reading in the House of Commons when a general election was called.

Since then, provincial governments, including British Columbia's, and various Canadian law enforcement agencies have made submissions urging the federal government to adopt lawful access measures. After consulting a broad range of stakeholders, including those from the telecommunications industry, civil liberty groups and victims' rights groups, the federal Minister of Public Safety introduced Bill C-47, which duplicates the fundamental provisions of the former Bill C-74.

2. International Context

Bill C-47 is a key step in the harmonization of legislation at the international level, particularly concerning requirements regarding the interception capabilities of telecommunications service providers. This type of requirement is already found in the legislation of a number of other countries, including the United States, the United Kingdom and Australia.(7)

Canada signed the Council of Europe's *Convention on Cybercrime* in November 2001, as well as its Additional Protocol on hate crime in July 2005. The Convention makes it an offence to commit certain crimes using computer systems and creates legal tools adapted to new technologies, such as orders to produce "subscriber information,"(8) which are similar to the

---

(6) See Nevis Consulting Group (General Editor), *Summary of Submissions to the Lawful Access Consultation*, Department of Justice Canada, 28 April 2003, http://canada.justice.gc.ca/eng/cons/la-al/sum-res/index.html.

(7) For more information on legislation in these countries, see Dominique Valiquet, *Telecommunications and Lawful Access: II. The Legislative Situation in the United States, the United Kingdom and Australia*, PRB 05-66E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 28 February 2006, http://lpintrabp.parl.gc.ca/LopImages2/prbpubs/bp1000/prb0566-e.asp.

(8) Council of Europe, *Convention on Cybercrime*, 23 November 2001, art. 18.

requests for subscriber information set out in Bill C-47. The injunction in the Convention does not specify whether subscriber information can be obtained without a warrant.

Complementary legislation in Bill C-46 includes other provisions, such as those concerning preservation and production orders and the modernization of offences related to computer viruses and hate propaganda, which will enable Canada to ratify the *Convention on Cybercrime* and the Additional Protocol.

DESCRIPTION AND ANALYSIS

A. Interception Capability (Clauses 6 to 15)

1. Current Situation

At present, no Canadian legislation compels all telecommunications service providers to use apparatus capable of intercepting communications. Only licensees that use radio frequencies for wireless voice telephony services have been required, since 1996, to have equipment that permits such interceptions.(9) There is no similar requirement for other telecommunications service providers.

2. Situation Under the Bill

This bill is designed to remedy the absence of standards for the interception capability of telecommunications service providers. It will require all service providers, including, for example, Internet service providers, to possess apparatus enabling law enforcement agencies, once they have obtained a judicial authorization, to intercept communications sent via the service provider. Within six months of the date on which the bill comes into force, telecommunications service providers will have to submit a report to the minister stating their capability to respond to the interception requirements set out in the bill (clauses 30 and 69).

---

(9) This requirement is imposed by Industry Canada when issuing spectrum licences under the *Broadcasting Act*. The rules governing interception are set out in the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications* (revised in November 1995). See Kirsten Embree, "Lawful Access: A Summary of the Federal Government's Recent Proposals – Part I," *Internet and E-Commerce Law in Canada*, Vol. 6, May 2005, p. 18, and Industry Canada, *Spectrum Management and Telecommunications*, "Personal Communications Services," http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf02092.html.

3. Obligations of Telecommunications Service Providers

a. The Capacity to Intercept Telecommunications (Clauses 6(1) and 7(*a*))

The requirement for interception capability relates both to "telecommunications data"[10] and to the actual content of the communication. Telecommunications service providers must use apparatus that enables law enforcement agencies to intercept, for example, subscribers' e-mail and Internet protocol (IP) addresses, the date and time of communications and the types of files transmitted (telecommunications data) and the substance of messages (content-related data).

b. Provision of Requested Information (Clauses 6(1) and 6(5))

Once a law enforcement agency has obtained a judicial authorization, the telecommunications service provider must provide all communications that have been intercepted (clause 6(1)). If possible, the telecommunications service provider must provide the intercepted communication in the form specified by the law enforcement agency (clause 6(5)). The service provider will also be required to give law enforcement agencies, on request, information relating to its facilities and the telecommunications services it offers (clause 6(1)(*b*) and clause 24).

c. Confidentiality (Clause 6(2))

All interception processes must be kept confidential. Telecommunications service providers are thus required to comply with the regulations and to guarantee the security of the contents of the intercepted communication, the telecommunications data and the identity of the individuals and organizations involved.

d. Decryption of Intercepted Communications (Clauses 6(3) and 6(4))

At present, wireless digital communications service providers have an obligation, under their operating licence conditions, to provide law enforcement agencies with decrypted communications. The bill extends that obligation to all technologies. However, if measures taken

(10) See the definition of "telecommunications data" at clause 2(1) of the bill. This means data that identify the origin, destination, date, time, duration, type and size of a telecommunication. This is also sometimes referred to as "traffic data." According to the proposed regulatory policy under the former Bill C-74, a telecommunications service provider lacking the ability to intercept telecommunications data in real time should at least have been capable of intercepting data within one second of intercepting the contents of the communication.

to protect a communication, such as encrypting or encoding, require the telecommunications service provider to develop specific decryption techniques or tools, the telecommunications service provider will not be required to decrypt the intercepted communication.

e. Isolation of the Intercepted Communication (Clause 7(*b*))

A judicial authorization to intercept communications will be made for one or more specific individuals. The telecommunications service provider must therefore be able to separate the communications of the person for whom the authorization is granted from the communications of other users. It must also have the capability to isolate the telecommunications data from the content-related data.

f. Correlation (Clause 7(*c*))

Telecommunications service providers must also have the technical capability to link telecommunications data to the content of an intercepted communication. This will allow the law enforcement agency to associate the offence committed with an IP address, for example.

g. Simultaneous Interceptions (Clause 7(*d*))

Telecommunications service providers are required to allow law enforcement agencies to intercept communications transmitted at the same time by more than one user.[11]

4. Entry Into Force of the Obligations (Clauses 10 and 11)

The bill does not require telecommunications service providers to meet the technical standards for interception capability as soon as the legislation comes into force. Rather, they must do so when updating their systems. Any transmission apparatus acquired or software installed after clauses 10 and 11 come into force must comply with the new standards. However, clause 67 provides that if the acquisition or installation takes place within the 18-month transition period following the coming into force of these two clauses, the application of

(11) Regulations will establish the minimum and maximum numbers of simultaneous interceptions that telecommunications facilities must be able to support (clauses 64(1)(*h*) and (*i*)). The minister may, however, order a service provider to take measures to increase the number of simultaneous interceptions to a number greater than the maximum (clause 14(1)(*b*)).

both clauses will be suspended until the end of the transition period.[12] For example, new software installed nine months after clause 11 comes into force need not comply with the new technical standards until nine months later, at the end of the transition period.

However, the minister will have the power, at the request of the Commissioner of the Royal Canadian Mounted Police (RCMP) or the Director of the Canadian Security Intelligence Service (CSIS), to issue a ministerial order requiring a telecommunications service provider, before upgrading, to acquire communications interception capability that meets the technical standards (clauses 14(1)(*d*) and (*e*)).

B. Requests for Subscriber Information (Clauses 16 to 23)

1. Current Situation

At present, law enforcement agencies need a warrant or court order to obtain personal information about clients from telecommunications service providers.[13]

2. Situation Under the Bill

The bill establishes special rules that enable designated people within law enforcement organizations to obtain basic information about a subscriber from a telecommunications service provider, without a warrant or court order.[14] The bill provides for protection measures in relation to such information requests.

---

(12) The former Bill C-74 provided for a 12-month transition period.

(13) See paragraph 7(3)(*c*) of the *Personal Information Protection and Electronic Documents Act*. However, the Ontario Superior Court of Justice ruled that subscribers do not have a reasonable expectation of privacy with respect to basic information held by their Internet service provider (*R.* v. *Wilson*, no. 4191/08, 10 February 2009; see also *R.* v. *Ward*, 2008 CarswellOnt 4728 (Ontario Court of Justice)). The Court found that a subscriber's name and address do not reveal intimate details of his or her lifestyle and personal choices (for more on the notion of "intimate details," see *R.* v. *Plant*, [1993] 3 S.C.R. 281). Previously, the Ontario Court of Justice had ruled otherwise in *R.* v. *Kwok*, [2008] O.J. 2414.

(14) The regulatory policy set out in the former Bill C-74 required designated people to at least provide an identifier associated with the subscriber to prevent "fishing expeditions." For example, to obtain a subscriber's name, the designated person would have to provide an IP address.

3. Request for Information

a. Types of Information That May Be Requested (Clause 16(1))

The information covered by the special rules is strictly limited. The bill lists the information associated with the subscriber's services and equipment that can be obtained without a warrant:

- name;
- address;
- telephone number;
- email address;
- Internet protocol address;
- mobile identification number;
- electronic serial number;
- local service provider identifier;
- international mobile equipment identity number;
- international mobile subscriber identity number; and
- subscriber identity module card number.(15)

Telecommunications service providers are not required to collect information other than the information they already collect in the normal course of business. The bill uses the expression "any information in the service provider's possession or control." As well, they are not required to verify the accuracy of the information they collect.

b. Designated Persons (Clauses 16(3) to 16(5))

Only a designated person may make a request for information under the bill. The person is designated by the Commissioner of the RCMP, the Director of CSIS, the Commissioner of Competition or a chief of police within their respective organizations and must perform duties related to protecting national security or to law enforcement (clause 16(3)).

(15) The definition of "subscriber information" in article 18 of the *Convention on Cybercrime* specifically excludes traffic data.

Each organization may designate a limited number of employees: a minimum of 5% of the agency's employees or, where an organization has 100 or fewer employees, five persons (clause 16(4)).

c. Urgent Situations: Request by a Police Officer (Clause 17)

In an urgent situation that it is reasonably believed may result in serious harm to a person or to property, a police officer – instead of the designated persons – may make a request for information (clause 17(1)).[16] The police officer must, however, inform a designated person in his or her organization, and that person will inform the telecommunications service provider of the request in writing (clauses 17(3) and (4)).

d. Purpose of Request (Clause 16(2))

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

e. Confidentiality (Clause 23)

The entire process surrounding the request for information remains confidential. The telecommunications service provider must not inform a subscriber that a designated person has made a request or that it has provided information to the designated person.

4. Protection Measures

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

---

(16) This refers to the same exceptional circumstances as those set out in s. 184.4 of the *Criminal Code*, relating to the interception of communications.

(17) For example, organizations may use the information obtained to lay criminal charges.

a. Records (Clause 18)

It must be possible to trace every request for information. The request must therefore be made in writing (clause 16(1)). Designated persons will also be required to keep a record that contains such details as the reasons for each request and the information obtained.

b. Internal Audits (Clauses 20(1), 20(2), 20(3), 20(7) and 20(8))

The Commissioner of the RCMP, the Director of CSIS, the Commissioner of Competition or a chief of police will be required to take measures to verify, on a regular basis, that the requests made by their organization comply with the provisions in Bill C-47 and its regulations. Among other things, the records and the use made of the information must therefore be examined. Reports concerning the results of the audits must be submitted to the responsible minister and, depending on the law enforcement agency that prepared the report, to the Privacy Commissioner of Canada, the Security Intelligence Review Committee or the provincial public officer responsible for privacy protection.

c. External Audits (Clauses 20(4) to 20(6))

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

C. Enforcement of Bill's Provisions (Clauses 33 to 38)

The minister may designate any person to verify compliance with the provisions of the bill. These individuals may enter any place owned by a telecommunications service provider to examine documents and telecommunications facilities in that place.

D. Violations and Offences (Clauses 39 to 63)

The bill provides for two types of contraventions: violations and offences. It establishes what is essentially a code of penal procedure for violations, which are apparently less serious contraventions. For offences, the summary conviction procedure set out in the *Criminal Code* applies. The bill sets out fines for both types of contraventions. No provision is made for imprisonment.

1. Violations

The Governor in Council will determine, by regulation, which contraventions of the bill constitute a violation (clause 39). The regulations will also establish the maximum fine that may be imposed for each violation. The amount of the fine may not exceed $50,000 in the case of an individual and $250,000 in the case of a corporation (clause 64(1)(*p*)(ii)).

2. Offences

The bill subdivides offences into four categories, based on the amount of the fine that may be imposed:

1. A breach of the obligations relating to capability to intercept, or contravention of a ministerial order, will be liable to maximum fines of $100,000 in the case of an individual and $500,000 in the case of a corporation (clause 55). In addition, if a telecommunications service provider does not have the required interception capability when its system is updated, a court may issue an injunction to prevent the use of transmission apparatus or software (clause 63).

2. Every person who makes a change to a law enforcement agency's interception equipment, fails to submit a report concerning interception capability, makes a false statement or fails to comply with the conditions of a suspension or exemption will be liable to a fine not exceeding $25,000 in the case of an individual ($50,000 for a subsequent offence) or $100,000 in the case of a corporation ($250,000 for a subsequent offence) (clause 56(1)).

3. Failure to cooperate with a designated person verifying compliance with the provisions of the bill or obstructing his or her work will constitute an offence punishable by a maximum fine of $15,000 (clause 56(2)).

4. Every person who contravenes other provisions in the bill will be liable to a maximum fine of $250,000,[18] if the offence in question is not designated by the regulations as a violation (clause 57).

It is important to note that the consent of the Attorney General of Canada is needed before a prosecution may be commenced in respect of the first two categories of offences (clause 58).

(18) For example, provisions relating to requests for subscriber information.

E. Exemptions (Clauses 5, 13, 32 and 68 and Schedules 1 and 2)

The bill will apply to all telecommunications service providers operating a transmission facility in Canada, subject to specified complete and partial exemptions in Schedules 1 and 2. However, the Governor in Council may amend these schedules by regulation to add or delete a class of telecommunications service providers (clause 5(4)). The bill also sets out temporary exemptions for maximum periods of two or three years, depending on the case.

1. Complete Exemptions

a. Private Networks (Clause 5(1), Part 1 of Schedule 1)

The bill contains no provisions that apply to private networks, which means persons who provide telecommunications services primarily to themselves, their household or their employees, and not to the public.

b. Sale or Purchase of Goods and Services (Clause 5(1), Part 1 of Schedule 1)

The bill will not apply to telecommunications service providers that provide telecommunications services intended principally for the sale or purchase of goods or services other than telecommunications services to the public.

c. Specified Institutions (Clause 5(1), Parts 1 and 2 of Schedule 1)

As well, no provision of the bill will apply in the case of:

- financial institutions;
- registered charities;
- educational institutions (except post-secondary institutions);
- hospitals;
- places of worship;
- retirement homes;
- telecommunications research companies; and
- broadcasters.

2. Partial Exemptions

a. Intermediary Telecommunications Service Providers (Clause 5(2), Part 1 of Schedule 2)

Telecommunications service providers that act as intermediaries, that is, that transmit communications on behalf of other telecommunications service providers without modifying communications or authenticating the users, will not be subject to the obligations regarding interception capability when they upgrade their systems or to the obligations in respect of subscriber information. However, they may be made subject to these by order of the minister (clause 14(2)).

b. Specified Institutions (Clause 5(3), Part 2 of Schedule 2)

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

- a post-secondary educational institution;
- a library;
- a community centre;
- a restaurant; or
- a hotel or apartment building.

3. Temporary Exemptions

a. Order Suspending Obligations (Clause 13)

The minister may, by order made on the application of a telecommunications service provider, suspend for up to three years, in whole or in part, any obligation relating to interception capability when systems are upgraded. The minister may include any conditions that he or she considers appropriate.

b. Exemption Regulation (Clause 32)

The Governor in Council may, on the recommendation of the minister and the minister of Industry, make a regulation exempting certain categories of telecommunications service providers from the most significant obligations in the bill, including obligations relating to interception capability when systems are upgraded or obligations relating to subscriber information. The exemption may impose conditions and may be valid for a maximum of two years.

c. Telecommunications Service Providers With Fewer Than 100,000 Subscribers (Clause 68)

The bill grants a three-year exemption for service providers with fewer than 100,000 subscribers. During that period, such small service providers will not have to comply with the interception capability standards required when systems are upgraded. However, they must provide a physical connection point permitting law enforcement agencies to intercept communications.

F. Compensation for Telecommunications Service Providers (Clauses 14(3), 21(1) and 29(1))

The bill provides for three situations in which the law enforcement agency must compensate a telecommunications service provider:

- The minister has made an order aimed at, for example, compelling the telecommunications service provider to comply with additional obligations related to interception capability (clause 14(3)).
- The telecommunications service provider has provided subscriber information at the request of the law enforcement agency (clause 21(1)).
- The telecommunications service provider has provided "specialized telecommunications support" to the law enforcement agency (clause 29(1)).

The definition of what constitutes "specialized telecommunications support," as well as the amount of and criteria for compensation will be determined by the regulations.(19)

G. Coming Into Force and Review of Act (Clauses 66 and 71)

The bill will come into force on a day or days set by order of the Governor in Council. Should the bill come into force on more than one day, different provisions would come into force at different times (clause 71).

The bill provides for parliamentary review of the enforcement of its provisions five years after the day on which it comes into force (clause 66).

(19) A recent Supreme Court of Canada ruling shed light on the matter of compensating a telecommunications service provider for costs associated with executing a production order for call data (s. 487.012 of the *Criminal Code*). The Court ruled that various factors should be taken into account, including the breadth of the order being sought, the size and economic viability of the object of the order, and the extent of the order's financial impact on the telecommunications service provider. (*Tele-Mobile Co.* v. *Ontario*, [2008] 1 S.C.R. 305).