LIBRARY of PARLIAMENT
BIBLIOTHÈQUE du PARLEMENT

LEGISLATIVE SUMMARY

Bill C-52:
Investigating and Preventing Criminal Electronic Communications Act

Publication No. 40-3-C52-E
30 May 2011

Erin Shaw
International Affairs, Trade and Finance Division

Dominique Valiquet
Legal and Legislative Affairs Division
Parliamentary Information and Research Service

Legislative Summary of Bill C-52

HTML and PDF versions of this publication are available on IntraParl (the parliamentary intranet) and on the Parliament of Canada website.

In the electronic versions, a number of the endnote entries contain hyperlinks to referenced resources.

Ce document est également publié en français.

Library of Parliament ***Legislative Summaries*** summarize government bills currently before Parliament and provide background about them in an objective and impartial manner. They are prepared by the Parliamentary Information and Research Service, which carries out research for and provides information and analysis to parliamentarians and Senate and House of Commons committees and parliamentary associations. Legislative Summaries are revised as needed to reflect amendments made to bills as they move through the legislative process.

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.

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

Publication No. 40-3-C52-E
Ottawa, Canada, Library of Parliament (2011)

CONTENTS

LEGISLATIVE SUMMARY OF BILL C-52: INVESTIGATING AND PREVENTING CRIMINAL ELECTRONIC COMMUNICATIONS ACT*

1 INTRODUCTION

On 1 November 2010, Bill C-52, An Act regulating telecommunications facilities to support investigations (short title: Investigating and Preventing Criminal Electronic Communications Act), was introduced in the House of Commons by the Minister of Public Safety (the Minister), the Honourable Vic Toews. It died on the *Order Paper* when the 40th Parliament was dissolved on 26 March 2011.

The bill deals with very specific aspects of the rules governing lawful access. Lawful access is an investigative technique used by law enforcement agencies and national security agencies that involves intercepting private communications[1] and seizing information where authorized by law. Rules and conditions 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*.[2]

Bill C-52 revives many of the essential provisions of two previous bills that died on the *Order Paper*. Bill C-74, the Modernization of Investigative Techniques Act, was introduced during the 1st session of the 38th Parliament in November 2005, and died on the *Order Paper* on 29 November 2005, when the 38th Parliament was dissolved. Bill C-47, the Technical Assistance for Law Enforcement in the 21st Century Act, was introduced during the 2nd session of the 40th Parliament in June 2009 and reproduced many of the fundamental provisions of the former Bill C-74. Bill C-47 later died on the *Order Paper* when Parliament was prorogued in December 2009.[3]

Bill C-52 addresses a concern expressed by law enforcement agencies 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 transmitted through their networks, regardless of the transmission technology used (clauses 6 to 15).
- It provides law enforcement and national security agencies with access to basic information about telecommunications service subscribers, under an accelerated and non-warrant- or court order-based administrative process. At the same time, the bill provides for certain safeguards (clauses 16 to 23).

Bill C-52 is part of a series of bills introduced during the 3rd Session of the 40th Parliament that aims to create a lawful access regime in Canada. This series includes:

- Bill C-51, the Investigative Powers for the 21st Century Act, which modernizes certain offences in the *Criminal Code* and the *Competition Act* to take into account new communications technologies and to provide new tools to law enforcement to investigate computer crimes.

- Bill C-50, the Improving Access to Investigative Tools for Serious Crimes Act, which amends *Criminal Code* provisions relating to the interception of private communications, tracking devices and telephone number recorders.[4]

A third, related piece of legislation is Bill C-29, the Safeguarding Canadians' Personal Information Act. Bill C-29 amends the *Personal Information and Electronic Documents Act* to broaden the range of purposes for which law enforcement authorities may request the provision of personal information from private entities without the consent of the individual concerned. The amendments also would expand the range of uses and permissible disclosure, without consent, by law enforcement of private information obtained under lawful authority, such as that provided under Bill C-52.[5]

In addition, amendments introduced in Bill C-29 and in Bill C-52 would restrict the circumstances under which individuals may be informed that the government has requested or received their personal information.[6]

1.1 Background

1.1.1 Cybercrime and Cybersecurity

Since 1995, law enforcement agencies have called for legislation that requires all telecommunications service providers to have technical means in place to enable police services to carry out lawful interceptions on their networks.

Currently, the procedures governing access to subscriber information held by Internet service providers (ISPs) are perceived by some to slow investigators' access to vital information in today's fast-paced, near-borderless digital world. It has been argued that the technical inability to isolate or intercept communications in real time may impede investigators and prosecutors. What is more, strong encryption techniques can prevent law enforcement and national security officials from accessing information unless they also have the power to access the decryption key.[7]

The Canadian national security community has argued that legislative amendments enabling reliable, fast and secure access to data held by telecommunications service providers, including subscriber information, are required in order for Canada to identify networked machines responsible for sophisticated cyber-attacks on strategic targets, and to actively defend valuable information and networks in Canada.[8]

1.1.2 National Consultations

Following the development of a strategic framework in 2000, officials from Justice Canada, Industry Canada and the Solicitor General of Canada[9] held public consultations in 2002.[10] A summary of the results of the consultations was made public in 2003 and Bill C-54, the Modernization of Investigative Techniques Act, was introduced in November 2005.[11] Further consultations were held by Public Safety Canada in 2007, including consultations with those from the telecommunications industry, civil liberty groups and victims' rights groups. The Minister of Public Safety

subsequently introduced Bill C-47, the Technical Assistance for Law Enforcement in the 21st Century Act.

Both Bill C-54 and Bill C-47 died on the *Order Paper*.

During and since the consultations, debate has centred on whether there is a need for lawful access legislation, the appropriate level of protection for individual privacy rights, and the propriety and costs of imposing technical interception standards on private businesses.[12]

1.1.3 International Obligations

Bill C-52 represents a step towards harmonizing the tools available to counter cybercrime at the international level, particularly regarding the interception capabilities of telecommunications service providers.[13] 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.[14] The Convention requires states that are party to the treaty to create offences under their domestic law criminalizing certain uses of computer systems, and requires the adoption of legal tools adapted to deal with new technologies, such as orders to produce "subscriber information."

The Convention does not specify the exact mechanisms that must be used to meet these obligations, leaving these choices up to the states that are party to the treaty. Such choices include determining whether a judicial warrant or other authorization is needed prior to accessing information. In addition, the domestic criminal procedures that states are required to adopt under the Convention relate only to law enforcement activities – the Convention does not require states to create procedural mechanisms permitting the interception of private communications and/or the disclosure of private information for broader national security purposes. Finally, the Convention requires states to respect all relevant national and international human rights obligations when implementing their obligations under the treaty.[15]

2 DESCRIPTION AND ANALYSIS

2.1 Interception Capability (Clauses 6 to 15)

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 permitting such interceptions.[16] There is no similar requirement for other telecommunications service providers.

Telecommunications service providers may legally intercept private communications in four cases:

- if the interception is pursuant to a court order;
- if the interception is reasonably necessary to preserve the quality and performance of a computer system;

- if it is necessary to protect a computer system against hacking and cyber-attacks; or
- if the communication's originator or intended recipient has given express or implied consent to the interception.[17]

In order to intercept the content of private communications, law enforcement and national security agencies require prior legal authorization, usually in the form of a judicial warrant.[18] Bill C-52 will not alter these requirements.

On the other hand, Bill C-52 requires all telecommunications service providers (including, for example, ISPs) to possess the technical capacity to allow law enforcement and national security agencies to intercept communications sent via the service provider, once the relevant legal authorization has been obtained.

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 70).

2.1.1 Obligations of Telecommunications Service Providers

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

Under Bill C-52, telecommunications service providers must use apparatus that enable law enforcement and national security agencies to intercept, for example, subscribers' email and Internet protocol (IP) addresses, the date and time of communications and the types of files transmitted (telecommunications data),[19] and the substance of messages (content-related data).

2.1.1.2 Provision of Requested Information (Clause 6)

Once a law enforcement or national security agency has obtained the necessary legal authorization, the telecommunications service provider must provide all communications that have been lawfully intercepted (clause 6(1)). If possible, the telecommunications service provider must provide the intercepted communication in the form specified by the requesting agency, which includes decrypted communications if the telecommunications service provider has the technical capacity to provide this. However, telecommunications service providers are not required to develop specific decryption techniques themselves (clauses 6(4) and 6(5)).

Bill C-52 requires that telecommunications service providers keep interception processes and requests confidential (clauses 6(2) and 23).

2.1.1.3 Operational Requirements for Telecommunications Service Providers (Clause 7)

A key feature of Bill C-52 is the requirement that all telecommunications service providers have specific technical capacities to allow them to intercept

communications transmitted through their networks. Specific capabilities required under the bill include:

- the ability to separate the communications of a specific person from the communications of other users, which is necessary because judicial warrants usually relate to a specific individual or individuals;
- the ability to isolate data that identifies the time, date, duration, size, destination, origin, etc. of a communication (telecommunications data) from the contents of the communication itself; and
- the capability to link telecommunications data to the content of an intercepted communication. This will allow a law enforcement or national security agency to associate the offence committed with an IP address, for example.

Telecommunications service providers also must have the capability to allow multiple law enforcement and national security agencies to intercept communications transmitted at the same time by more than one user.[20]

2.1.2 Compliance (Clauses 10 and 11)

The bill requires telecommunications service providers to meet the new technical standards for interception when updating their systems. Thus, any transmission apparatus acquired or software installed after clauses 10 and 11 come into force must comply with the new standards. In other words, there is no requirement under the bill for a service provider to update systems simply to comply with the new standards. However, at the request of the Commissioner of the Royal Canadian Mounted Police (RCMP) or the Director of the Canadian Security Intelligence Service (CSIS), the Minister has the power to order a telecommunications service provider, before upgrading, to acquire communications interception capability that meets the new technical standards (clauses 14(1)(*d*) and (*e*)).

2.2 Requests for Subscriber Information (Clauses 16 to 23)

2.2.1 Current Situation

At present, in most circumstances, private organizations must disclose personal information about clients to law enforcement and national security agencies, without the consent of the individual concerned, only if the relevant agency has judicial or other legal authorization to compel the production of the information. In other circumstances, the disclosure of personal information is not mandatory. In practice, telecommunications service providers in Canada tend to disclose clients' personal information voluntarily only in circumstances permitted under their subscriber agreements, and generally only in order to minimize an imminent danger to life or property.[21]

Recent legislation has, however, imposed a requirement that ISPs report pro-actively to police if they have reasonable grounds to believe that the services they provide are being used to transmit child pornography.[22]

The legality of police requests for voluntary disclosure of subscriber information by telecommunications service providers (disclosure in the absence of a warrant) has been an issue before the courts, challenged as a violation of the right to be free from unreasonable search or seizure under section 8 of the *Canadian Charter of Rights and Freedoms*, which protects individual privacy from intrusion by the state. The Supreme Court of Canada has held that individuals have a reasonable expectation of privacy in information that tends to reveal intimate details about their lifestyle and personal choices.[23] Judicial decisions as to whether a warrant is needed to access subscriber information, therefore, generally turn on whether the individual concerned had a reasonable expectation of privacy in such information.

Whether individuals currently have a reasonable expectation of privacy in subscriber information remains somewhat unclear and the case law is highly fact-specific. A number of lower court decisions have held that subscribers do not have a reasonable expectation of privacy in relation to such information.[24] However, a reasonable expectation of privacy has been found in certain other cases.[25] Recent case law suggests that the more that subscriber information tends to reveal patterns of use of telecommunications equipment that could expose intimate details about lifestyle or personality, the greater the likelihood that individuals would have a reasonable expectation of privacy in that information.[26]

Bill C-52 aims to provide clarity with respect to the types of information that may be disclosed to law enforcement or national security agencies without a warrant.

2.2.2 Provisions of the Bill

Bill C-52 establishes a process that enables designated people within law enforcement and national security organizations to request and obtain certain subscriber information from a telecommunications service provider, without a warrant or other legal authorization (clause 16(1)).[27] The bill also establishes certain safeguards.

2.2.2.1 Information That May Be Requested (Clause 16)

Only specific types of information associated with the subscriber's services and equipment can be obtained without a warrant:

- name;
- address;
- telephone number;
- email address;
- IP 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.[28]

The bill does not require telecommunications service providers to gather information other than that already collected in the normal course of business. Nor are they required to verify the accuracy of this information (for example, the accuracy of a subscriber's name or postal address).

2.2.2.2 Designated Persons (Clause 16)

Requests for subscriber information may be made, in writing, only by individuals who perform duties related to the protection of national security or law enforcement, and who are designated by the Commissioner of the RCMP, the Director of CSIS, the Commissioner of Competition or their chief of police ("designated persons") (clause 16(3)).

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

2.2.2.3 Purposes for Which Information May Be Sought (Clauses 16 and 19)

Designated members of police services may request, in writing, information that relates to any police function, including the enforcement of any federal or provincial laws, or the laws of a foreign state. Designated members of CSIS and the Commissioner of Competition may only request information relating to their functions under their relevant enabling legislation (clause 16(2)).

Information obtained through these requests can be used only for the purposes above, or for a use consistent with these purposes, unless the individual in question has given consent to broader use (clause 19).[29] Service agreements between telecommunications service providers and customers, which normally are contracts of adhesion,[30] could incorporate a consent clause allowing for broader uses of information obtained pursuant to the bill.[31]

2.2.2.4 Exceptional Circumstances: Request by a Police Officer (Clause 17)

All police officers, whether or not they are designated persons under the bill, would have the power to require the disclosure of subscriber information by telecommunications service providers in urgent situations if:

- they have reasonable grounds to believe that they cannot, with due diligence, make a request under the normal procedures;

- they have reasonable grounds to believe that the information is needed immediately to prevent an unlawful act that would result in serious harm to a person or to property; and
- the information directly concerns either the expected perpetrator of the act or the victim/intended victim (clause 17(1)).[32]

Subsequently, a designated person at the same agency must provide a written record of the request to the telecommunications service provider (clauses 17(3) and (4)).

2.2.3 AUDITS (CLAUSE 20)

Requests for information must be made in writing, and the reasons for the request and the information obtained must be recorded (clause 18).

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 respective organization comply with the provisions in Bill C-52 and its regulations (clause 20(1)).

If the relevant agency head or police chief is of the opinion that anything arising out of his or her audit should be brought to the attention of the responsible minister, he or she must report the information and any corrective action proposed or taken without delay (clause 20(2)). Therefore, the bill establishes a subjective standard for reporting.

Depending on the agency in question, the audit report also must be provided to an independent review body: the Privacy Commissioner of Canada (in the case of the RCMP or the Commissioner of Competition), the Security Intelligence Review Committee (in the case of CSIS) or the provincial public officer responsible for privacy protection (in the case of a provincial or municipal police service). There is no requirement that reports be furnished to other provincial accountability bodies that have review and/or oversight functions in relation to municipal or provincial police forces (clause 20(3)).

The Privacy Commissioner of Canada and the Security Intelligence Review Committee have the power to conduct external reviews of requests for subscriber information provided for in the bill (clauses 20(4) to 20(5)). The Privacy Commissioner also must report annually on the powers of provincial privacy officers to conduct external audits in relation to provincial and municipal police forces (clause 20(6)). Currently, not all provincial privacy officers have the power to conduct the type of external audits envisioned in the bill.[33]

There is no specific power in the bill authorizing the RCMP Public Complaints Commission, which has the power to initiate investigations into the conduct of any member of the RCMP or other person employed under the *Royal Canadian Mounted Police Act*, to access all information related to internal or external audits. The RCMP Complaints Commission currently does not have the power to compel the production

of information or documents, unless a public hearing is held in relation to a specific complaint.[34]

2.3 Enforcement Provisions (Clauses 33 to 38)

The Minister may designate any person to verify compliance with the provisions of the bill. Such individuals may enter any place owned by a telecommunications service provider to examine documents, information and telecommunications facilities; use computer systems to search and examine information; or use any other telecommunications device in that location. However, if the place in question is a dwelling house – a structure that is occupied as a permanent or temporary residence – then a designated person must obtain a judicial warrant in order to first gain access.[35] Without obtaining a judicial warrant, designated persons may create and remove copies of any information found, and are authorized to enter and pass through private property, other than a dwelling house, in order to exercise these powers (examples of such privately owned property could include office buildings, stores, yards, etc.) (clauses 34, 35 and 36).

Telecommunications service providers must provide all necessary assistance during such compliance visits (clauses 34(3), 38).

2.3.1 Violations and Offences (Clauses 39 to 63)

The bill provides for two types of contraventions: violations and offences. The scheme of the bill suggests that violations are considered to be less serious infractions than offences. The bill sets out fines for both types of contraventions. No provision is made for imprisonment.

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. Fines range up to $50,000 in the case of an individual and up to $250,000 in the case of a corporation or any other entity (clause 64(1)(*p*)(ii)).

An administrative procedure allows persons served with notices of violation to dispute their liability by making representations to a person designated by the Minister (clause 43). Decisions made under this procedure may be appealed to the Minister (clause 44(1)) and the Minister's decision on appeal is subject to judicial review.[36]

The summary conviction procedure set out in the *Criminal Code* applies to offences, with fines ranging between $15,000 and $250,000 for an individual and between $15,000 and $500,000 for a corporation. The bill provides for four categories of offences (clauses 55, 56(1), 56(2), 57):

- Breach of the obligations relating to capability to intercept, or contravention of a ministerial order. These offences will be liable to maximum fines of $100,000 in the case of an individual and $500,000 in the case of a corporation or other entity (clause 55).

- Alteration of a law enforcement agency's interception equipment; failure to submit a report concerning interception capability; making a false statement; or, failure to comply with the conditions of a suspension or exemption. These offences will be liable to fines 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 or any other entity ($250,000 for a subsequent offence) (clause 56(1)).
- Failure to cooperate with a designated person verifying compliance with the provisions of the bill or obstructing his or her work. Such failures will constitute offences punishable by a maximum fine of $15,000 (clause 56(2)).
- Contravention of other provisions in the bill. These offences will be punishable by a maximum fine of $250,000,[37] unless the offence in question is designated by the regulations as a violation (clause 57).

The consent of the Attorney General of Canada is needed before a prosecution may be initiated in respect of the first two categories of offences (clause 58).

2.4 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 contained in Schedules 1 and 2. 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.

2.4.1 Complete Exemptions (Clause 5(1), and Parts 1 and 2 of Schedule 1)

The bill does not apply to private networks; that is, to persons who provide telecommunications services primarily to themselves, their household or their employees, and not to the public. Nor will the bill 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. Finally, the provisions of the bill will not apply to the core functions of financial institutions, registered charities, educational institutions (except post-secondary institutions), hospitals, places of worship, retirement homes, telecommunications research companies, and broadcasters.

2.4.1.1 Partial Exemptions (Clauses 5(2) to (3), and Parts 1 and 2 of Schedule 2)

Post-secondary educational institutions, libraries, community centres, restaurants, hotels, condominiums and apartment buildings will be required to provide information about their telecommunications facilities to law enforcement agencies, but will not be subject to the other obligations under the bill.

Telecommunications service providers that transmit communications on behalf of other telecommunications service providers without modifying communications or

authenticating the users (known as intermediaries) will not be subject to the obligations regarding interception capability, unless they are made subject to these requirements by order of the Minister (clauses 14(1), 14(2)).

2.4.1.2 Temporary Exemptions (Clauses 13, 32 and 69)

The bill provides the Minister with the power to exempt telecommunications service providers from any obligation relating to interception capability, on application by the provider. The bill also allows the Governor in Council to create regulations that exempt certain categories of telecommunications providers from significant obligations, including those relating to interception capability and subscriber information. Both types of exemptions may be subject to conditions and may be valid for up to three years (clauses 13, 32).

The bill also grants a three-year exemption for service providers with fewer than 100,000 subscribers. However, they must provide a physical connection point permitting law enforcement agencies to intercept communications (clause 69).

2.5 Compensation for Telecommunications Service Providers (Clauses 14, 21 and 29)

The bill provides for three situations in which a law enforcement or national security 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 or national security agency (clause 21(1)).
- The telecommunications service provider has provided "specialized telecommunications support" to the law enforcement or national security agency (clause 29(1)).

The definition of what constitutes "specialized telecommunications support," as well as the amount of and criteria for compensation, will be set out in the regulations.[38]

2.6 Coming into Force and Review of Act (Clauses 67 and 71 to 73)

The bill contains a number of coordinating amendments that would have come into force had bills C-29 and C-50 also been passed by Parliament (clauses 71, 72).

The bill provides for parliamentary review of the enforcement of its provisions five years after the day on which it comes into force (clause 67).

NOTES

* Holly Porteous, analyst in the International Affairs, Trade and Finance Division, Library of Parliament, contributed to this legislative summary.

1. Commonly called "wiretapping."

2. *Criminal Code*, R.S.C. 1985, c. C-46; Canadian Security Intelligence Service Act, R.S.C. 1985, c. 23; *National Defence Act*, R.S.C. 1985, c. N-5.

3. For more information about these bills, see Dominique Valiquet, *Telecommunications and Lawful Access: I. The Legislative Situation in Canada*, Publication No. 05-65-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 21 February 2006.

4. For more information about these bills, see Dominique Valiquet, *Legislative Summary of Bill C-50: An Act to amend the Criminal Code (interception of private communications and related warrants and orders)*, Publication no. 40-3-C50-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 9 November 2010; and Dominique Valiquet and Katherine Simonds, *Legislative Summary of Bill C-51: Investigative Powers for the 21st Century Act*, Publication no. 40-3-C51-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 3 February 2011.

5. Bill C-29, An Act to amend the Personal Information Protection and Electronic Documents Act, 3rd Session, 40th Parliament, clauses 6(6) and 6(13). See also clause 6(12). For more information on Bill C-29, see Alysia Davies, *Legislative Summary of Bill C-29: An Act to amend the Personal Information Protection and Electronic Documents Act*, Publication no. 40-3-C29-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 23 June 2010.

6. See Bill C-52, clause 71; Bill C-29, clause 8. For more information on Bill C-29, see Davies (2010).

7. See, for example, Canadian Association of Chiefs of Police, Resolutions #06-2007, "Lawful Access to Encrypted Electronic Media," *Resolutions Adopted at the 102nd Annual Conference*, Calgary, August 2007, p. 26.

8. See Public Policy Forum, *Cyber Security: Developing a Canadian Strategy*, Ottawa, 27 March 2008; Canadian Association of Chiefs of Police, *Resolutions* (August 2007); Holly Porteous, "Cybersecurity and Intelligence: The US Approach," Publication no. 2010-02E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 8 February 2010; and Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age," *Canadian Criminal Law Review,* Vol. 12, 2008, p.115. For international perspectives on similar problems in other countries, see U.S., Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing before the House of Representatives Committee on Judiciary Subcommittee on Crime, Terrorism, and Homeland Security, 112th Cong. (17 February 2011) (Valerie Caproni, General Counsel, Federal Bureau of Investigation); and Council of Europe, *Explanatory Report to the Convention on Cybercrime (E.T.S. No. 185)*, n.d., para. 219.

9. The Solicitor General's ministry was renamed the Ministry of Public Safety and Emergency Preparedness in 2003. The post of Solicitor General was formally abolished in 2005.

10. See Department of Justice Canada, Industry Canada and Solicitor General Canada, *Lawful Access – Consultation Document*, Ottawa, 25 August 2002.

11. See Nevis Consulting Group Inc. (General Editor), *Summary of Submissions to the Lawful Access Consultation*, Department of Justice Canada, Ottawa, 28 April 2003.

12. For examples, see Privacy Commissioner of Canada, Information and Privacy Commissioner of Alberta, Information and Privacy Commissioner for British Columbia et al., "Letter to Public Safety Canada from Canada's Privacy Commissioners and Ombudspersons on the current 'Lawful Access' proposals," 9 March 2011; "Chapter 6: Comments by Civil Society Groups," Summary of Submissions to the Lawful Access Consultation, Department of Justice Canada, 28 April 2003; Canadian Wireless Telecommunications Association, "Letter," 12 October 2007, p. 2; and Michael Geist, "Geist: Lawful access legislation would reshape Canada's Internet," *Toronto Star*,16 November 2010.

13. For more information on foreign lawful access legislation, see Dominique Valiquet, *Telecommunications and Lawful Access II: The Legislative Situation in the United States, the United Kingdom and Australia*, Publication no. 05-66E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 28 February 2006.

14. *Convention on Cybercrime*, 23 November 2001, Eur.T.S. 185, art. 18 (in force 1 July 2004); *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, 28 January 2003, Eur. T.S. 189 (in force 1 March 2006).

15. *Convention on Cybercrime*, arts. 14(1)–(2), 15 and Preamble; Council of Europe, *Explanatory Report to the Convention on Cybercrime*, paras. 5, 135, 145–148, 182, 210–215, 221–225, 230. For an overview of some of the debates around lawful access legislation in other countries, see U.S., *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies:* Hearing before the House of Representatives Committee on Judiciary Subcommittee on Crime, Terrorism, and Homeland Security, 112th Cong., 17 February 2011 (Susan Landau, Fellow, Radcliffe Institute for Advanced Study, Harvard University); Declan McCullagh, "Police Want Backdoor to Web Users' Private Data," *CNET News*, 3 February 2010; U.K., House of Lords, Select Committee on the Constitution, *Surveillance: Citizens and the State*, Vol. I: Report, 2nd Report of Session 2008–09, HLP-18-I, 6 February 2009, pp. 11–29; and Germany, Federal Constitutional Court, "Data retention unconstitutional in its present form – Judgment of 2 March 2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08," Press Release No. 11/2010, 2 March 2010

16. This requirement is imposed by Industry Canada when issuing spectrum licences under the *Radiocommunication Act*, R.S.C. 1985, c. R-2. The rules currently 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; Industry Canada, "Personal Communications Services," *Spectrum Management and Telecommunications*; and for an example, see Industry Canada, "Notice No. DGRB-004-09 - Decision on the Renewal of 24 and 38 GHz Spectrum Licences and Consultation on Spectrum Licence Fees for 24, 28 and 38 GHz Bands, Annex A – Conditions of Licence," *Spectrum Management and Telecommunications*, March 2009, para 9.

17. *Criminal Code*, s. 184(2)(a), (e). Note that if the originator or recipient of a communication works for or with law enforcement, a judicial warrant would be required for the interception to be lawful.

18. The interception of "private communications" is governed by Part VI of the *Criminal Code*, ss. 183–196. The Canadian Security Intelligence Service may obtain judicial authorization to intercept communications under the *Canadian Security Intelligence Service Act*, ss. 21–28. Interceptions of communications by the Communications Security Establishment that are not directed at Canadians or any person in Canada are permitted by ministerial authorizations under s. 273.65 of the *National Defence Act*. Such authorizations allow the interception of private communications only for the purpose of gathering "information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international

affairs, defence or security" (*National Defence Act,* s. 273.61). The Communications Security Establishment may also "provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties" (*National Defence Act*, s. 273.64(1)(*c*)).

19. See the definition of “telecommunications data” in clause 2(1) of the bill, which defines telecommunications data as data that identify the origin, destination, date, time, duration, type and size of a telecommunication. Telecommunications data 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 have been capable, at a minimum, of intercepting data within one second of intercepting the contents of the communication.

20. 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*)).

21. Information Technology Association of Canada, *Customer Name and Address Consultation*, Mississauga, October 2007, p. 1. For examples, see Bell Canada, Bell Internet Service Agreement – effective October 1, 2010, clauses 13, 17; Rogers Communications Inc., Rogers Terms of Service, n.d., clauses 19, 29.

22. Sections 2–4 of *An Act respecting the Mandatory Reporting of Internet Child Pornography by Persons who Provide an Internet Service*, S.C. 2011, c. 4, in force 28 March 2011.

23. *R.* v. *Plant*, [1993] 3 S.C.R. 281, p. 293. See also the recent Supreme Court decision in *R.* v. *Gomboc*, [2010] 3 S.C.R. 211.

24. *R.* v. *McNeice*, 2010 BCSC 1544 (B.C.S.C.); *R.* v. *Brousseau*, 2010 ONSC 6753 (Ont. S.C.J.) (where disclosure permitted by subscriber agreement); *R.* v. *Vasic* (2009), 185 C.R.R. (2d) 286 (Ont. S.C.J.) (where disclosure permitted by subscriber agreement); *R.* v. *Wilson*, [2009] O.J. No. 1067, 10 February 2009 (Ont. S.C.J.); *R.* v. *Spencer*, 2009 SKQB 341 (Sask. Q.B.); *R.* v. *Ward*, 2008 CarswellOnt 4728 (Ont. C.J.); *R.* v. *Verge*, 2009 CarswellOnt 501 (Ont. C.J.); *R.* v. *Trapp* (2009), 330 Sask. R. 169 (Sask. Prov. Ct.).

25. *R.* v. *Nguyen* (2004), 20 C.R. (6th) 135 (B.C.S.C.); *R.* v. *Mahmood* (2008), 236 C.C.C. (3d) 3 (Ont. S.C.J.); *R.* v. *Kwok*, [2008] O.J. 2414; (Ont. C.J.); *R.* v. *Cuttell*, 2009 ONCJ 471, 247 C.C.C. (3d) 424 (Ont. C.J.).

26. For example, see *R.* v. *Gomboc*, paras. 100–104 (per Chief Justice McLachlin and Justice Fish).

27. 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.

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

29. For example, organizations may use the information obtained to lay criminal charges.

30. A contract of adhesion is a contract that is presented in a standard form by one party, where the terms are neither negotiated nor negotiable.

31. Current Bell and Rogers service agreements contain standard clauses authorizing disclosure of confidential personal information necessary to public authorities if there is an imminent danger to life or property that could be avoided by disclosure of the information, or to satisfy existing laws or regulations. The service agreements also give the providers the right to monitor and investigate content or a subscriber's use of the

provider's networks: Bell Canada (1 October 2010), clauses 13, 17; Rogers Communications Inc. (n.d.), clauses 19, 29.

32. 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.

33. Privacy Commissioner of Canada, Information and Privacy Commissioner of Alberta, Information and Privacy Commissioner for British Columbia et al., "Letter to Public Safety Canada from Canada's Privacy Commissioners and Ombudspersons on the current 'Lawful Access' proposals," 9 March 2011.

34. *Royal Canadian Mounted Police Act*, R.S.C. 1985, c. R-10, ss. 45.37, 45.42, 45.43 and 45.45(4). The RCMP Police Complaints Commission does not have the power to compel the RCMP Commissioner to produce information or documents outside of the public hearing process. For a discussion of the sufficiency of the powers of the RCMP Public Complaints Commission, see Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities*, Public Works and Government Services Canada, Ottawa, 2006, pp. 244–252, 483–494 and 514–558; Task Force on Governance and Cultural Change within the RCMP, Rebuilding the Trust: Task Force on Governance and Cultural Change within the RCMP, Ottawa, December 2007, pp. 11–23; Jennifer Stoddart, Privacy Commissioner of Canada, *Rights and reality: enhancing oversight for national security programs in Canada – Office of the Privacy Commissioner of Canada's Submission to the Standing Committee on Public Safety and National Security – Review of the Findings and Recommendations of the Internal Inquiry into the Actions of Canadian Officials in relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin (Iacobucci Inquiry) and the report from the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (Arar Inquiry)*, Ottawa, 7 May 2009. Bill C-38, An Act to amend the Royal Canadian Mounted Police Act and to make consequential amendments to other Acts, 3rd Session, 40th Parliament, which died on the *Order Paper* in March 2011, would have created a new RCMP Review and Complaints Commission with expanded powers to conduct reviews of the propriety of RCMP activities (clause 8). For more information, see Lyne Casavant and Dominique Valiquet, *Legislative Summary of Bill C-38: An Act to amend the Royal Canadian Mounted Police Act and to make consequential amendments to other Acts*, Publication No. 40-3-C38-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 24 September 2010.

35. The term "dwelling house" is defined in section 2 of the Criminal Code.

36. *Federal Courts Act*, R.S.C. 1985, c. F-7, s. 18.1. It is well-established that section 18.1 applies to the exercise of Ministerial discretion. See, for example, *Canada* v. *Addison & Leyen Ltd.*, [2007] 2 S.C.R. 793.

37. For example, the provisions relating to requests for subscriber information.

38. 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.