LIBRARY of PARLIAMENT
BIBLIOTHÈQUE du PARLEMENT

LEGISLATIVE SUMMARY

Bill C-30:
An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts

Publication No. 41-1-C30-E
15 February 2012

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-30

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. 41-1-C30-E
Ottawa, Canada, Library of Parliament (2012)

CONTENTS

LEGISLATIVE SUMMARY OF BILL C-30: AN ACT TO ENACT THE INVESTIGATING AND PREVENTING CRIMINAL ELECTRONIC COMMUNICATIONS ACT AND TO AMEND THE CRIMINAL CODE AND OTHER ACTS

1 BACKGROUND

On 14 February 2012, Bill C-30, An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts (short title: Protecting Children from Internet Predators Act) was introduced in the House of Commons by the Minister of Public Safety, the Honourable Vic Toews.

1.1 PURPOSE OF THE BILL

Bill C-30 deals with "lawful access." Lawful access is an investigative technique used by law enforcement agencies and national security agencies that involves intercepting private communications and seizing information where authorized by law.

Bill C-30 basically groups together the provisions of former bills C-50, C-51 and C-52, which were introduced in the 3rd Session of the 40th Parliament and which all died on the *Order Paper* before second reading in the House of Commons. The structure of Bill C-30 follows that of these former bills: Part 1 enacts a new law governing "telecommunications service providers," (former Bill C-52); and Part 2 amends the *Criminal Code* and other Acts respecting the interception of private communications (former Bill C-50), the modernization of certain offences and the creation of new investigative tools tailored to computer crime (former Bill).

Bill C-30 should be read in conjunction with Bill C-12, which also deals with lawful access. Bill C-12 amends the *Personal Information Protection and Electronic Documents Act* to expand the number of circumstances in which law enforcement agencies can ask private organizations to voluntarily provide them with personal information without consent.[1]

1.2 MAIN AMENDMENTS IN THE BILL

Part 1 of Bill C-30 addresses a concern expressed by law enforcement agencies that new technologies, particularly Internet communications, often present obstacles to lawful communications interception. The bill creates the *Investigating and Preventing Criminal Electronic Communications Act* (IPCECA), which 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 (sections 6 to 15 of the IPCECA).
- 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 (sections 16 to 23 of the IPCECA).

Part 2 of the bill aims to update Canadian criminal law. More specifically, the principle amendments in the bill:

- provide that if an authorization to intercept communications is given, a related warrant, such as a search warrant, may be issued at the same time (clauses 8, 10 and 12 of the bill);
- require the government to report annually on the interceptions of private communications made without authorizations and notify individuals who have been the object of an interception (clauses 13 and 14 of the bill);
- extend the scope of hate propaganda offences to protect individuals distinguished by national origin or mental or physical disability (clause 16 of the bill);
- create the offence of possession of a computer virus for the purpose of committing mischief (clause 21 of the bill);
- make it possible for law enforcement agencies to make a demand or obtain a court order for the preservation of electronic evidence (clause 24 of the bill);
- create new judicial production orders for obtaining data relating to the transmission of communications or data for tracking a thing or individual (clause 24 of the bill);
- create warrants for obtaining transmission data in real time and for the remote activation of "tracking devices"[2] in certain types of technologies (clause 28);
- modernize the deceptive marketing practices offences in the *Competition Act* (clauses 35 and 37 of the bill); and
- amend the *Mutual Legal Assistance in Criminal Matters Act* so the new production orders can be used by Canadian authorities who receive assistance requests from other countries (clause 43 of the bill).

1.3 Main Differences with Former Bills on Lawful Access

There are a few differences between Bill C-30 and former bills C-50, C-51 and C-52. For example, Bill C-30:

- restricts the *type of information* that can be obtained without a warrant (section 16 of the IPCECA);
- specifies that the request for subscriber information by a police officer in an emergency may be done *orally or in writing* (section 17 of the IPCECA);
- provides as a safeguard an *objective* standard of responsibility (section 20(2) of the IPCECA);
- unlike former Bill C-51, does not expressly provide that hate propaganda offences may be committed by *any means of communication* and includes *making available* hateful material (clause 5 of former Bill C-51); and
- provides that the maximum duration of a preservation order is *90 days* in the case of an offence committed under a law of a foreign state (clause 24 of the bill, new section 487.012(4) of the Code).

1.4 Legislative Background and National Consultations

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.[3]

Following the development of a strategic framework in 2000, officials from Justice Canada, Industry Canada and the Solicitor General of Canada[4] held public consultations in 2002.[5] A summary of the results of the consultations was made public in 2003,[6] and a bill on lawful access was introduced in November 2005: Bill C-74 (Modernization of Investigative Techniques Act).

Further consultations were held by Public Safety Canada in 2007, including consultations with representatives of the telecommunications industry, civil liberty groups and victims' rights groups. In 2009, Bill C-47 (Technical Assistance for Law Enforcement in the 21st Century Act), which contained the key provisions of former Bill C-74, was introduced at the same time as a brand new bill on lawful access: Bill C-46 (Investigative Powers for the 21st Century Act). To these two bills – which were introduced again in 2010 in the following legislative session as bills C-51 and C-52 – a third was added: Bill C-50 (Improving Access to Investigate Tools for Serious Crimes Act). All these bills on lawful access died on the *Order Paper* before being passed.

According to a Public Safety Canada news release, at the January 2012 meeting in Charlottetown of federal, provincial and territorial ministers responsible for justice and public safety:

> the ministers unanimously agreed on the need to enhance and modernize the investigative capability of law enforcement and urged the federal government to move forward on enacting previously introduced legislation.[7]

Since the 2002 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.[8]

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.[9]

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 protect valuable information and networks in Canada.[10]

1.5 International Obligations

Bill C-30 represents a step towards harmonizing the tools available to counter cybercrime at the international level, particularly regarding production orders, orders for the preservation of computer data and the interception capabilities of telecommunications service providers.[11] 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.[12] The Convention requires states that are parties to the treaty to create offences under their domestic laws 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." It seems, then, that Bill C-30 would allow Canada to ratify the Convention and its Additional Protocol. However, one might ask whether the bill goes further than required by the Convention.

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 parties to the treaty. Such choices include determining whether a warrant or other judicial 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 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.[13]

2 Description and Analysis

2.1 Part 1 (Clauses 2 to 5)

Part 1 of the bill creates a new act: the *Investigating and Preventing Criminal Electronic Communications Act* (IPCECA).

2.1.1 Interception Capability (Sections 6 to 15 of the IPCECA)

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.[14] 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 for the interception.[15]

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.[16] Bill C-30 will not alter these requirements.

On the other hand, once the relevant legal authorization has been obtained, all telecommunications service providers (including, for example, ISPs) will be required, under Bill C-30, to possess the technical capacity to allow law enforcement and national security agencies 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 (clause 5).

2.1.1.1 Obligations Imposed on Telecommunications Service Providers When Updating

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 sections 10 and 11 of the IPCECA 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 (secton 14 of the IPCECA).

In addition, Bill C-30 provides a transition period of 18 months during which obligations respecting interception capability are suspended (clause 3). However, the minister may order a telecommunications service provider to comply with these obligations during the transition period (section 14 of the IPCECA).

2.1.1.2 Capability to Intercept Telecommunications Data and Content (Sections 6(1) and 7(*a*) of the IPCECA)

Under Bill C-30, telecommunications service providers must use apparatuses that enable law enforcement and national security agencies to intercept such elements as subscribers' email and Internet protocol (IP) addresses, the date and time of communications and the types of files transmitted ("telecommunications data"),[17] as well as the content of messages (content-related data).

2.1.1.3 Confidential Communication of Decrypted Information (Section 6 of the IPCECA)

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 (section 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 (sections 6(4) and 6(5)).

Bill C-30 requires that telecommunications service providers keep interception procedures and requests confidential (sections 6(2) and 23).

2.1.1.3.1 Operational Requirements for Apparatuses (Section 7 of the IPCECA)

New telecommunications apparatuses must permit the interception of communications transmitted over the networks of telecommunications service providers and have the capability to do the following:

- 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;
- isolate data that identifies the date, time, duration, size, destination, origin, etc., of a communication ("telecommunications data") from the contents of the communication itself; and
- link telecommunications data to the content of an intercepted communication. For example, this would allow a law enforcement or national security agency to connect the offence committed with an IP address.

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.

2.1.2 Requests for Subscriber Information (Sections 16 to 23 of the IPCECA)

2.1.2.1 Current Situation

At present, in most circumstances,[18] private organizations (like ISPs) must disclose personal information about clients to law enforcement and national security agencies, without the consent of the individual(s) concerned, only if the relevant agency has judicial or other legal authorization to compel the production of the information. As the disclosure of personal information is not mandatory, the organization has the choice to *voluntarily* disclose this information. In practice, telecommunications service providers in Canada tend to disclose clients' personal information voluntarily only in circumstances permitted under their service contract, and generally only in order to minimize an imminent danger to life or property.[19]

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 the privacy of the individual from intrusion by the state. The Supreme Court of Canada has held that individuals have a reasonable expectation of privacy regarding information that reveals intimate details about their lifestyle and personal choices.[20] Judicial decisions as to whether a warrant is needed to access subscriber information, therefore, generally turn on whether the individual concerned could have a reasonable expectation of privacy regarding such information.

Whether individuals currently have such an expectation regarding subscriber information remains somewhat unclear, and the case law is fact-specific. A number of lower court decisions have held that subscribers cannot have a reasonable expectation of privacy in relation to such information.[21] However, a reasonable expectation of privacy has been found in certain other cases.[22] Recent case law suggests that it is more reasonable to expect respect for privacy when subscriber information can reveal computer equipment use habits that could expose intimate details about lifestyle or personality.[23]

Bill C-30 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.

2.1.2.2 Provisions of the IPCECA

Bill C-30 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 (section 16(1)). A number of safeguards are also built into this process.

2.1.2.2.1 Information that May Be Requested (Section 16 of the IPCECA)

Pursuant to the bill, only six types of information concerning telecommunications subscribers may be obtained without a warrant:

- name;
- address;
- telephone number;
- email address;
- IP address;[24] and
- local service provider identifier.

Bill C-30 seems, then, to provide a more limited list of information than that established by former Bill C-52. The list in the former bill, in addition to the six types

of information listed above, included information associated with the subscriber's equipment: the mobile identification number; electronic serial number (ESN); international mobile equipment identity number (IMEI); international mobile subscriber identity number (IMSI); and subscriber identity module card number (SIM).

Another difference respecting former Bill C-52 relates to the content of a written request made by a designated person: Bill C-30 expressly provides that, to obtain one of the six types of information, the police officer or CSIS agent must provide the telecommunications service provider with "identifying information." The meaning of "identifying information" will be defined later by regulation (section 64(1)(*l*) of the IPCECA). Hypothetically, a police officer will have to provide an IP address to a telecommunications service provider in order to obtain the subscriber's name and physical address.

Moreover, 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).

2.1.2.2.2 Designated Persons (Section 16 of the IPCECA)

In general, 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 Office of the Commissioner of Competition or their chief of police ("designated persons") (section 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 (section 16(4)).

2.1.2.2.3 Purposes for Which Information May Be Sought (Sections 16 and 19 of the IPCECA)

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

Information obtained through these requests can be used only for the purposes outlined above, or for a use consistent with these purposes, unless the individual in question has given consent to broader use (section 19).[25] Service agreements between telecommunications service providers and customers, which normally are contracts of adhesion,[26] could incorporate a consent clause allowing for broader uses of information obtained pursuant to the bill.[27]

2.1.2.2.4 Exceptional Circumstances: Request by Any Police Officer (Section 17 of the IPCECA)

Police officers, whether designated persons or not under the bill, have the power to ask, orally or in writing, that telecommunications service providers disclose subscriber information without a warrant in urgent situations in the following circumstances:

- 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 suspected perpetrator of the act or the victim or intended victim (section 17(1)).[28]

Subsequently, a designated person from the same agency as the officer must provide a written account of the request to the telecommunications service provider (sections 17(3) and (4)).

2.1.2.2.5 Safeguards: Audits (Sections 18 and 20 of the IPCECA)

Requests for information must be made in writing, and the reasons for any request and the information obtained must be recorded (section 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-30 and its regulations (section 20(1)). *In each case*, they must then, without delay, report on the findings of this internal audit to the responsible minister (section 20(2)). Former Bill C-52 provided only for a subjective standard of reporting: the person who caused an internal audit to be conducted would have been required to make a report only when, *in the person's opinion*, the audit revealed something that should be brought to the attention of the responsible minister.

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 (section 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 (sections 20(4) to 20(5)). The Privacy Commissioner also must report annually on the powers of provincial public officers to conduct external audits in relation to provincial and municipal police forces (section 20(6)). Currently, not all provincial privacy officers have the power to conduct the type of external audits envisioned in the bill.[29]

There is no specific power in the bill authorizing the RCMP Public Complaints Commission, which has the power to initiate an investigation 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.[30]

2.1.3 Administration and Enforcement of the IPCECA (Sections 33 to 38 of the IPCECA)

The minister may designate any person an "inspector" to verify compliance with the provisions of the IPCECA. The inspector 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 (sections 34 and 36).

The inspector may, without a judicial warrant, photocopy and remove copies of any information found, and, in order to exercise these powers, enter and pass through private property, other than a dwelling-house (examples of such privately owned property could include office buildings, stores, yards, etc.). If the place in question is a dwelling-house – a structure that is occupied as a permanent or temporary residence – the inspector must obtain a judicial warrant in order to gain access without the occupant's consent (section 35). Telecommunication service providers must give all assistance that is required during these visits to verify compliance (sections 34(3) and 38).

2.1.4 Violations and Offences in the IPCECA (Sections 39 to 63 of the IPCECA)

The IPCECA provides for two types of contraventions: violations and offences; violations are considered to be less serious infractions than offences. The IPCECA 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* (section 39). The regulations will also establish the maximum fine that may be imposed for each violation. Fines may be as high as $50,000 in the case of an individual and $250,000 in the case of a corporation or any other entity.

An administrative procedure allows persons served with notices of a *violation* to dispute their liability by making representations to a person designated by the minister (section 43). Decisions made under this procedure may be appealed to the minister (section 44(1)), and the minister's decision on appeal is subject to judicial review.[31]

The summary conviction procedure set out in the *Criminal Code* applies to *offences*, with fines of 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 (sections 55, 56(1), 56(2), 57):

- Breach of the obligations relating to the capability to intercept, or contravention of a ministerial order. Fines for these offences can reach $100,000 in the case of an individual and $500,000 in the case of a corporation or other entity (section 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. The fines for these offences are not to exceed $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) (section 56(1)).

- Failure to cooperate with an inspector 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. The fines in these cases can reach $250,000,[32] unless the offence in question is designated by the regulations as a violation (section 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 (section 58).

2.1.5 Telecommunications Service Providers Subject to the IPCECA and Exemptions

The IPCECA 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 provider (section 5(4)). The bill also sets out temporary exemptions for maximum periods of two or three years, depending on the case.

2.1.5.1 Complete Exemptions (Section 5(1) of and Schedule 1 to the IPCECA)

The IPCECA 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.

2.1.5.2 Partial Exemptions (Sections 5(2) and 5(3) of and Schedule 2 to the IPCECA)

Post-secondary educational institutions, libraries, community centres, restaurants, hotels, condominiums and apartment buildings will be required to provide information about their telecommunications facilities to national security and 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 (sections 14(1) and 14(2)).

2.1.5.3 Temporary Exemptions (Sections 13 and 32 of the IPCECA and Clause 4 of the Bill)

The IPCECA provides the minister with the power to exempt telecommunications service providers from any obligation relating to interception capability, on application by the provider (section 13). It 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. These two types of temporary exemptions may be subject to conditions and may be valid for up to three years and two years, respectively (section 32).

The bill also grants a three-year exemption for telecommunication service providers with fewer than 100,000 subscribers. However, these service providers must provide a physical connection point permitting national security and law enforcement agencies to intercept communications (clause 4 of the bill).

2.1.6 Compensation for Telecommunications Service Providers (Sections 14, 21, 29 and 66 of the IPCECA)

The IPCECA 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 (section 14(3)).
- The telecommunications service provider has provided subscriber information at the request of the law enforcement or national security agency (section 21(1)).
- The telecommunications service provider has provided “specialized telecommunications support” to the law enforcement or national security agency (section 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.[33]

2.1.7 Parliamentary Review of the IPCECA (Section 67 of the IPCECA)

The IPCECA provides for parliamentary review of the enforcement of its provisions five years after the day on which it comes into force.

2.2 PART 2 (CLAUSES 6 TO 47 OF THE BILL)

Part 2 of Bill C-30 amends the *Criminal Code*, the *Competition Act* and the *Mutual Legal Assistance in Criminal Matters Act* to modernize criminal offences, legal instruments and provisions respecting the interception of private communications.

2.2.1 AMENDMENTS TO THE *CRIMINAL CODE*

2.2.1.1 INTERCEPTION OF PRIVATE COMMUNICATIONS

Part VI of the Code ("Invasion of Privacy," section 183 and following) is the centrepiece of federal legislation on electronic surveillance by law enforcement agencies. Respecting the interception of the contents of oral communications or video footage and often involving a serious invasion of privacy, Part VI sets out stricter conditions for the issuance of a judicial authorization to intercept private communications than for the granting of a search warrant or a production order.[34]

While Code provisions regarding search and seizure were amended in the 1980s and 1990s to expressly include computers, most provisions in Part VI date back to 1974.

2.2.1.1.1 AUTHORIZATIONS TO INTERCEPT AND RELATED WARRANTS (CLAUSES 8, 10, 11 AND 12 OF THE BILL)

Police forces often use electronic surveillance in conjunction with other investigative techniques. Given that an application for judicial authorization to intercept communications is sometimes based on the same information as that presented in support of an application for a warrant – a search warrant for example – or may come from the same source, the bill allows the judge to give an authorization to intercept communications and, at the same time, issue the requested warrant.

Regardless of whether the interception is done with the consent of one of the parties to the communication (section 184.2 of the Code), without the consent of the parties (sections 185 and 186 of the Code) or for a maximum period of 36 hours in an emergency (section 188 of the Code), the judge can, in addition to giving an authorization to intercept, issue a search warrant, make an assistance order or issue a warrant to use a tracking device or a "transmission data recorder" (clauses 8, 10 and 12 of the bill). In cases other than emergencies (i.e., when sections 184.2, 185 or 186 apply), the judge can issue a general warrant, make a general production order or make a specific production order to obtain certain information, such as computer data or financial information (clauses 8 and 10 of the bill). In each case, these clauses allow police officers to more quickly investigate past or possible offences.

All documents relating to an application for authorization to intercept communications are confidential; that is why they are placed in a packet sealed by the judge (section 187 of the Code). Clause 11 of the bill provides that all documents relating to a request for a related warrant or order in connection with an authorization are subject to the same rules as an authorization to intercept, that is, they are kept secret, generally until the trial.

2.2.1.1.2 Interception of Communications Without Judicial Authorization (Clauses 9, 13 and 14 of the Bill)

Currently, a peace officer can, pursuant to section 184.4 of the Code, intercept private communications without judicial authorization if the following conditions are met: (i) there are reasonable grounds to believe that the urgency of the situation is such that an authorization could not be obtained; (ii) an immediate interception is necessary to prevent an *unlawful act* that would cause serious harm to a person or to property; (iii) one of the parties to the communication is the originator or victim or intended victim of the *unlawful act*. The expression *unlawful act* is not defined elsewhere in the Code.

Clause 9 of the bill limits, to a certain extent, the scope of section 184.4 by replacing "unlawful act" with "offence," which is defined in section 183 of the Code.[35] Therefore, the interception of communications without authorization in the exceptional circumstances set out in section 184.4 is not permitted except in regard to the offences set out in section 183, as is the case for most other types of interception under Part VI.

Section 195 of the Code currently requires the federal minister of public safety and the attorney general of each province to prepare an annual report on the use by police forces of warrants for video surveillance and certain authorizations to intercept private communications pursuant to Part VI: authorizations to intercept communications without the consent of the parties to the communication (sections 185 and 186 of the Code) and authorizations valid for a maximum period of 36 hours in emergencies (section 188 of the Code).

Clause 13 of the bill extends the requirement to present a public report on interceptions without judicial authorization made in exceptional circumstances set out in section 184.4 of the Code. The clause also sets out the new information to be included in the report. However, other types of interception and electronic surveillance set out in the Code are still not subject to the requirement for governments to present a public report on their use: interception to prevent bodily harm without judicial authorization (section 184.1), interception with the consent of one of the parties to the communication (section 184.2) and use of a tracking device (section 492.1) or "number recorder" (section 492.2).

Lastly, as with interception without consent but with judicial authorization (sections 185 and 186 of the Code), clause 14 of the bill provides that, in the case of an interception without judicial authorization in exceptional circumstances set out in section 184.4 of the Code, the federal minister of public safety or the attorney general of a province must notify the person who was the object of the interception, generally within 90 days of the interception. On application to a judge, this period may be extended to three years if the police investigation is continuing (section 196 of the Code). As is currently the case, this extension may be obtained more readily if the investigation relates to a terrorism or organized crime offence.

2.2.1.2 Modernization of Offences

2.2.1.2.1 Hate Propaganda (Clauses 15 and 16 of the Bill)

Hate propaganda offences must be committed against an "identifiable group." Respecting the offence of advocating genocide, clause 15 of the bill adds "national origin" to the definition of "identifiable group."[36] Clause 16 of the bill, which applies to the offences of public incitement to hatred and of wilful promotion of hatred, adds mental or physical disability to this definition, in addition to national origin.

2.2.1.2.2 Device for Theft of Telecommunication Services (Clause 19 of the Bill)

At present, section 327 of the Code makes it a crime to possess, manufacture or sell a device used for the theft of telecommunication services. Clause 19 of the bill essentially adds importing such a device or making it available. As well, the bill makes this indictable offence a hybrid offence; that is, the prosecutor will have the option of proceeding by indictment or summary conviction.

2.2.1.2.3 Computer Virus (Clause 21 of the Bill)

Under the existing provisions of the Code, only spreading or attempting to spread a computer virus[37] constitutes an offence.[38] In accordance with the requirements of the *Convention on Cybercrime*,[39] clause 21 of the bill makes it illegal to possess a computer virus for the purpose of committing mischief, and also makes it an offence to import and make available a computer virus.

2.2.1.2.4 False, Indecent or Harassing Communications (Clause 22 of the Bill)

The existing provisions of the Code regarding the offences of sending a message in a false name and sending false information, indecent remarks or "harassing" messages (the French term *harassants* currently used in subsection 372(3) of the Code is replaced by *harcelants* in the bill) refer to certain communication technologies used to commit those offences, such as telegram, radio and telephone.[40] Clause 22 of the bill amends those offences by removing the references to those specific communications technologies and, for some of those offences, substituting a reference to any means of telecommunication. As a result, it will be possible to lay charges regardless of the transmission method or technology used.

Additionally, the bill provides that the offences consisting of transmitting false information, indecent remarks or harassing messages will now be hybrid offences. Accordingly, the maximum sentence for the offences relating to indecent and harassing communications will be increased to imprisonment for two years, in the event that the prosecutor decides to proceed by indictment.

2.2.1.3 New Investigative Tools

2.2.1.3.1 Preservation Demand and Order (Clause 24 of the Bill)

Information in electronic form may be easily and quickly destroyed or altered. Clause 24 of the bill therefore adds a new investigative tool to the Code to preserve this type of evidence. This tool may take one of two forms: a preservation demand or a preservation order. A preservation demand is made by a peace officer (new section 487.012 of the Code), while a preservation order is made by a judge, on application by a peace officer (new section 487.013 of the Code).

A preservation demand or order directs a person, such as a telecommunications service provider, to preserve "computer data"[41] that are "in their possession or control" when they receive the demand or order. However, a telecommunications service provider may still *voluntarily* preserve data and provide it to a law enforcement agency, even where there is no demand or order (new section 487.0195 of the Code).

This new investigative tool is different from the data retention measure in effect in some countries,[42] which compels telecommunications service providers to collect and retain data for a prescribed period for all their subscribers, whether or not they are the subjects of an investigation. On the other hand, a preservation demand or order relates only to a particular telecommunication or person, in the context of a police investigation. A preservation demand or order may be given to a telecommunications service provider only where there are "reasonable grounds to suspect"[43] that an offence has been or will be committed (new sections 487.012(2) and 487.013(2) of the Code). However, the person who is suspected of the offence may not be compelled to retain data under a preservation demand or order (new sections 487.012(3) and 487.013(5) of the Code).[44]

Preservation demands and orders are temporary measures: they are generally in effect long enough to allow the law enforcement agency to obtain a search warrant or production order. The maximum length of a preservation demand is 21 days (in the case of an offence committed under federal law) or 90 days (in the case of an offence committed under a law of a foreign state), and the demand may be made only once (new sections 487.012(4) and 487.012(6) of the Code); the maximum length of a preservation order is 90 days (new section 487.013(6) of the Code).

A person who receives a preservation demand or order is required, after the demand or order expires, or after the data have been given to the law enforcement agency under a production order or search warrant, to destroy the computer data that would not be retained in the ordinary course of business (new sections 487.0194 and 487.0199 of the Code).

Contravention of a preservation demand is an offence punishable by a fine of not more than $5,000 (new section 487.0197 of the Code). Contravention of a preservation order is an offence punishable by a fine of not more than $250,000 or imprisonment for a term of not more than six months, or both (new section 487.0198 of the Code).

2.2.1.3.2 Production Orders (Clause 24 of the Bill)

A production order is made by a judge and is similar to a search warrant, the difference being that the person in possession of the information must produce it on request, rather than the law enforcement agency's going to the site to obtain the information by searching and seizing it. A law enforcement agency with a production order will be able to more readily obtain documents that are in another country, for example.

The Code already provides 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.[45] Issuance of the order is based on the existence of *reasonable grounds to believe* that an offence has been committed. The Code also provides for *specific* production orders, that is, orders for obtaining certain precise information, such as banking information or telephone call logs.[46] Issuance of specific production orders is based on the less stringent *reasonable grounds to suspect* that an offence has been or will be committed.

Clause 24 of the bill creates new specific production orders, issuance of which is based on the existence of reasonable grounds to suspect that an offence has been or will be committed, which allow a peace officer to obtain two types of information from a telecommunications service provider:[47] "transmission data" (new section 487.016 of the Code) and "tracking data" (new section 487.017 of the Code).[48]

Essentially, "transmission data" are data that indicate the origin, destination, date, time, duration, type and volume of a telecommunication (e.g., a telephone call or Internet communication), but do not include the content of the telecommunication.[49] The definition of "transmission data" is in this way similar to the definition of "telecommunications data" in Part 1 of Bill 30 creating the IPCECA. This type of data is useful: for example, it may be used to trace all telecommunications service providers involved in the transmission of data in order to identify the initial telecommunications service provider and thus determine the origin of a telecommunication (new section 487.015 of the Code). "Tracking data" relate to the location of a thing or individual.

These new production orders allow law enforcement agencies to obtain *historical* transmission or tracking data, that is, data already in the possession of the telecommunications service provider when it receives the order. To obtain these types of data *in real time*, law enforcement agencies need a warrant.

A review procedure is provided for challenging any type of production order, existing or new (new section 487.0193 of the Code).[50] A person who has received an order may apply to a judge to revoke or vary it if production is unreasonable[51] or discloses privileged information.[52] In the case of a preservation order, violation of a production order is punishable by a fine of not more than $250,000 or imprisonment for a term of not more than six months, or both (new section 487.0198 of the Code).

2.2.1.3.3 Warrant for a Tracking Device (Clause 28 of the Bill)

At present, section 492.1 of the Code allows a peace officer with a warrant,[53] to secretly install a tracking device (e.g., a GPS device) on a thing, if there are reasonable grounds to suspect that an offence has been or will be committed and

that information that would assist in the police investigation, notably the whereabouts of a person, can be obtained through the use of such a tracking device.

Clause 28 of the bill retains this type of warrant, but makes a distinction between a warrant to install a tracking device on a *thing*, such as a vehicle, to track its movements (new section 492.1(1) of the Code) and a warrant to install that kind of device on a thing *usually carried or worn by an individual*, such as a cellphone, in order to track the individual's location and movements (new section 492.1(2) of the Code). A warrant to track the movements of a thing is based on the existing standard of *reasonable grounds to suspect* that an offence has been or will be committed, while a more stringent standard applies to a warrant to track the movements of an individual: the existence of *reasonable grounds to believe* that an offence has been or will be committed.

In addition to allowing a tracking device to be *installed*, the bill allows law enforcement agencies to *remotely activate* devices of the kind that are found in certain types of technology, such as cellphones or the GPS devices in certain cars (new section 492.1(3) of the Code).

The maximum duration of a warrant for a tracking device is still 60 days. However, that period is extended to one year in the case of a terrorism organized crime offence (new section 492.1(5) and 492.1(6) of the Code).[54]

2.2.1.3.4 Warrant for a Transmission Data Recorder (Clause 28 of the Bill)

At present, subsection 492.2(1) of the Code allows a peace officer with a warrant to secretly install a number recorder on a telephone or telephone line, if there are reasonable grounds to suspect that an offence has been or will be committed and that information that would assist in the police investigation could be obtained through the use of this kind of recorder. The law enforcement agency could thus obtain the "incoming" and "outgoing" telephone numbers for a telephone that was being tapped.

Clause 28 of the bill provides for a warrant that authorizes a peace officer to install and activate a transmission data recorder[55] (new section 492.2 of the Code). As before, the warrant will allow law enforcement agencies to obtain telephonic data, but also to obtain data indicating the origin and destination of an Internet communication, for example. Police services will thus be able to have access to these transmission data in real time. As well, as in the case of a warrant to install a telephone number recorder, the new warrant is based on the requirement that there are reasonable grounds to suspect that an offence has been or will be committed. Lastly, clause 26 provides for the use of a transmission data recorder without a warrant in emergencies.

2.2.2 Amendments to the *Competition Act*

2.2.2.1 Preservation and Production Orders (Clause 31 of the Bill)

The new provisions of the Code concerning demands and orders for the preservation of computer data and orders for the production of transmission data and banking information will apply to certain investigations under the *Competition Act*. The Commissioner of Competition will thus be able to use these new investigative tools to obtain evidence relating to deceptive marketing practices and restrictive trade practices.

2.2.2.2 Modernization of Offences (Clauses 35 to 37 of the Bill)

Clauses 35 to 37 of the bill modernize certain offences related to deceptive marketing practices offences, such as deceptive telemarketing and making misrepresentations about a product or service, and replace the reference to "telephone" as the means of committing these offences with "any means of telecommunication" used for communicating orally.

2.2.3 Amendments to the *Mutual Legal Assistance in Criminal Matters Act*

The *Mutual Legal Assistance in Criminal Matters Act* was enacted in 1988 and gives Canadian courts the power to issue compulsory measures, such as subpoenas and search warrants, to obtain evidence in Canada on behalf of a foreign state for use in a criminal investigation and prosecution being conducted by that state. The legislation aims to promote cooperation among states by establishing a system for exchanging information and evidence.[56]

2.2.3.1 Searches by the Commissioner of Competition (Clause 39 of the Bill)

The bill authorizes the Commissioner of Competition to execute search warrants issued under the *Mutual Legal Assistance in Criminal Matters Act*.

2.2.3.2 Production Orders (Clause 43 of the Bill)

The bill provides that the production orders for obtaining banking information, transmission data or tracking data described in the Code may be used by Canadian authorities who receive assistance requests from their international partners.

NOTES

1. *Bill C-12: An Act to amend the Personal Information Protection and Electronic Documents Act*, 1st Session, 41st Parliament, sections 6(6) and 6(12). For more information about Bill C-12, see Dara Lithwick, *Legislative Summary of Bill C-12: An Act to amend the Personal Information Protection and Electronic Documents Act*, Publication no. 41-1-C12-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 19 October 2011.

2. New s. 492.1(8) of the *Criminal Code* defines "tracking devices" as devices that may be used to record or transmit tracking data in real time.

3. See, for example, Canadian Association of Chiefs of Police, "Simplifying Lawful Access: Bill C-30 – Through the Lens of Law Enforcement," 2012; and Canadian Association of Chiefs of Police, "Lawful Access Reform: A Position Paper Prepared for the Canadian Association of Chiefs of Police," 2008.

4. 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.

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

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

7. Public Safety Canada, "Harper government introduces *Protecting Children from Internet Predators Act*," News release, Ottawa, 14 February 2012.

8. For examples, see Privacy Commissioner of Canada, "Letter to Minister of Public Safety Vic Toews," 26 October 2011; 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; Michael Geist, "How to Fix Canada's Online Surveillance Bill: A 12-Step To-Do List," 24 February 2012; Christopher Parsons, "The Issues Surrounding Subscriber Information in Bill C-30," 28 February 2012; Danika J. Grenier, "C-30 a 'wide open' surveillance bill, provides access to telcos' data centres: Experts," *The Wire Report*, 22 February 2012; Danika J. Grenier, "Telcos still concerned about unknown costs of lawful access bill," *The Wire Report*, 21 February 2012; Tim Naumetz, "Human rights lawyer warns feds' internet surveillance bill could lead to massive internet sweep," *The Hill Times*, 22 February 2012; Philippa Lawson, *Moving Toward A Surveillance Society: Proposals to Expand "Lawful Access" In Canada*, BC Civil Liberties Association, 2012; Information and Privacy Commissioner of Ontario, *Beware of "Surveillance by Design": Standing up for Freedom and Privacy*; Department of Justice Canada, "Chapter 6: Comments by Civil Society Groups," *Summary of Submissions to the Lawful Access Consultation*, 28 April 2003; and Canadian Wireless Telecommunications Association, "Letter," 12 October 2007, p. 2.

9. See Canadian Association of Chiefs of Police, Resolutions no. 06-2007, "Lawful Access to Encrypted Electronic Media," *Resolutions Adopted at the 102nd Annual Conference*, Calgary, August 2007, p. 26.

10. 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 U.S. 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; and The Dark Space Project, *Final Report*, Bell Canada, 2011. For international perspectives on similar problems in other countries, see United States, *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, Hearing before the House of Representatives Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security, 112th Congress, 17 February 2011 (Valerie Caproni, General Counsel, Federal Bureau of Investigation); and Council of Europe, *Convention on Cybercrime: Explanatory Report*, E.T.S. No. 185, n.d., para. 219.

11. For more information on international lawful access legislation, see Christopher Parsons, *Lawful Access and Data Preservation/Retention: Present Practices, Ongoing Harm, and Future Canadian Policies*, 7 February 2012.

12. *Convention on Cybercrime*, 23 November 2001, E.T.S. No. 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, E.T.S. No. 189 (in force 1 March 2006).

13. *Convention on Cybercrime*, arts. 14(1) and (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 United States (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; United Kingdom, House of Lords, Select Committee on the Constitution, *Surveillance: Citizens and the State*, Vol. I: Report, 2nd report of session 2008–2009, 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.

14. 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.

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

16. 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*)).

17. See the definition of "telecommunications data" in c. 2(1) of the bill, which defines telecommunications data as data that identify the origin, type, direction, date, time, duration, size, destination or termination of a telecommunication generated or received by means of a telecommunications facility or the type of telecommunications service used. It also includes "transmission data," which applies to Part 2 of Bill C-30. The *Convention on Cybercrime* uses a different term: "traffic data."

18. An exception is provided by *An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service*, S.C. 2011, c. 4 (in force since 28 March 2011), which imposes a requirement that ISPs contact the police themselves if they have reasonable grounds to believe that the services they provide are being used to transmit child pornography.

19. In almost 95% of cases, ISPs voluntarily provide information requested by the RCMP (Sarah Schmidt, "Tories stand firm on 'online spying' legislation," *Postmedia News*, 13 February 2012). See also the Information Technology Association of Canada, *Customer Name and Address Consultation*, Mississauga, Ont., October 2007, p. 1. For examples of service agreements, see Bell Canada, *Bell Internet Service Agreement – effective October 1, 2010*, clauses 13 and 17; and Rogers Communications Inc., *Rogers Terms of Service*, n.d., clauses 19 and 29.

20. *R.* v. *Plant*, [1993] 3 S.C.R. 281, p. 293; *R.* v. *Tessling*, [2004] 3 S.C.R. 432; *R.* v. *Gomboc*, [2010] 3 S.C.R. 211.

21. *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.).

22. *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.).

23. See, for example, *R.* v. *Gomboc*, paras. 100–104 (per Chief Justice McLachlin and Justice Fish).

24. The definition of "subscriber information" in article 18 of the *Convention on Cybercrime* specifically excludes traffic data, which includes IP addresses (*Convention on Cybercrime*, Explanatory Report, para. 30).

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

26. 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.

27. 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 (2010), clauses 13 and 17; Rogers Communications Inc. (n.d.), clauses 19 and 29.

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

29. Privacy Commissioner of Canada (9 March 2011).

30. *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; and 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.

31. *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.

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

33. 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.

34. For more information on electronic surveillance, 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.

35. See the offences listed in section 183 of the *Criminal Code* under the definition of "offence." This list includes a large number of offences and continues to grow as new legislation relating to criminal law adds offences to the Code.

36. Under the present definition in the *Criminal Code*, s. 318(4), "identifiable group" means any section of the public distinguished by colour, race, religion, ethnic origin or sexual orientation." The definition in article 2 of the *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* also includes national origin. Article 20 of the Protocol's Explanatory Report reads as follows: "The notion of 'national origin' is to be understood in a broad factual sense. It may refer to individuals' histories, not only with regard to the nationality or origin of their ancestors but also to their own national belonging, irrespective of whether from a legal point of view they still possess it. When persons possess more than one nationality or are stateless, the broad interpretation of this notion intends to protect them if they are discriminated on any of these grounds. Moreover, the notion of 'national origin' may not only refer to the belonging to one of the countries that is internationally recognised as such, but also to minorities or other groups of persons, with similar characteristics."

37. In this legislative summary, the term "computer virus" includes other malicious code, such as computer worms.

38. *Criminal Code*, s. 430(1.1). See also s. 342.2.

39. *Convention on Cybercrime*, art. 6.

40. *Criminal Code*, ss. 371 and 372.

41. The definition of "computer data" is given in clause 20(4) of the bill. Essentially, it means data that can be processed by computer.

42. See European Parliament, *Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, 15 March 2006.

43. The *reasonable grounds to suspect* that an offence has been or will be committed requirement is less stringent than the usual requirement, *reasonable grounds to believe* that an offence has been or will be committed. Although the *reasonable grounds to suspect* requirement is also rarer, it is currently provided in certain other provisions of the *Criminal Code*.

44. Similarly, production orders may not compel the suspect in an investigation to disclose information (see the *Criminal Code*, new ss. 487.014 to 487.018).

45. *Criminal Code*, s. 487.012 (see also new s. 487.014, added by the bill, which provides for a similar general production order).

46. *Criminal Code*, ss, 487.013(1), 487.013(4) (see also new s. 487.018, added by the bill) and s. 492.2(2).

47. The peace officer may also obtain this information from another person – but not the suspect in a police investigation – who has the data in his or her possession or control.

48. See the definitions of these types of data in the *Criminal Code*, new s. 487.011, added by the bill.

49. Article 1 of the *Convention on Cybercrime* contains a similar definition, but uses the term "traffic data."

50. A similar procedure is currently provided in s. 487.015 of the *Criminal Code*.

51. See note 33.

52. A production order may contain conditions to protect information covered by solicitor–client privilege (*Criminal Code*, new s. 487.019(1), added by the bill).

53. Where there are exigent circumstances and the conditions for obtaining a warrant exist, a warrant is not necessary. The same is true for a search and a transmission date recorder (*Criminal Code*, s. 487.11; see also c. 26 of the bill).

54. This lengthened duration of the warrant is consistent with the current situation relating to wiretapping for terrorism and organized crime offences (*Criminal Code*, s. 186.1).

55. See the definition in new s. 492.2(6) of the *Criminal Code*.

56. This information comes from Department of Justice, Chapter 43, "Mutual Legal Assistance in Criminal Matters," in Part VIII, "International Assistance," *The Federal Prosecution Service Deskbook*.