LIBRARY of PARLIAMENT
BIBLIOTHÈQUE du PARLEMENT

LEGISLATIVE SUMMARY

Bill C-51:
Investigative Powers for the 21st Century Act

Publication No. 40-3-C51-E
3 February 2011

Dominique Valiquet

Legal and Legislative Affairs Division
Parliamentary Information and Research Service

Katherine Simonds

International Affairs, Trade and Finance Division
Parliamentary Information and Research Service

Legislative Summary of Bill C-51

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-C51-E
Ottawa, Canada, Library of Parliament (2011)

CONTENTS

LEGISLATIVE SUMMARY OF BILL C-51: INVESTIGATIVE POWERS FOR THE 21ST CENTURY ACT

1 BACKGROUND

1.1 PURPOSE OF THE BILL

Bill C-51: An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act (short title: Investigative Powers for the 21st Century Act) was introduced in the House of Commons on 1 November 2010 by the Minister of Justice, the Honourable Robert Douglas Nicholson, together with Dave MacKenzie, Parliamentary Secretary to the Minister of Public Safety and Daniel Petit, Parliamentary Secretary to the Minister of Justice.

The purpose of the bill is to modernize certain offences in the *Criminal Code* (the Code) and the *Competition Act* to take into account new communications technologies and to equip law enforcement agencies with new investigative tools that are adapted to computer crimes. To facilitate collaboration with foreign law enforcement agencies, the bill also amends the *Mutual Legal Assistance in Criminal Matters Act*. According to the Department of Justice, the new investigative powers within the proposed legislation give law enforcement agencies the ability to address organized crime and terrorism activities online by:

- enabling police to identify all the network nodes and jurisdictions involved in the transmission of data and trace the communications back to a suspect. Judicial authorizations would be required to obtain transmission data, which provides information on the routing but does not include the content of a private communication;
- requiring a telecommunications service provider to temporarily keep data so that it is not lost or deleted in the time it takes law enforcement agencies to return with a search warrant or production order to obtain it;
- making it illegal to possess a computer virus for the purposes of committing an offence of mischief; and
- enhancing international cooperation to help in investigating and prosecuting crime that goes beyond Canada's borders.[1]

Bill C-51 is identical to Bill C-46, introduced in the House of Commons during the 2nd Session of the 40th Parliament on 18 June 2009, with the exception that it does not contain provisions related to offences against children. Such provisions are proposed in this parliamentary session in Bill C-54, An Act to amend the Criminal Code (sexual offences against children).[2] The proposed legislation complements Bill C-52, An Act regulating telecommunications facilities to support investigations, and Bill C-50, An Act to amend the Criminal Code (interception of private communications and related warrants and orders), as these bills address different aspects of a proposed lawful access regime.[3]

1.2 Principal Amendments in the Bill

The bill aims to update Canadian criminal law. More specifically, the principal amendments in the bill:

- provide that hate propaganda offences can be committed by any means of communication and including making hate material available (clause 5);
- create the offence of possession of a computer virus for the purpose of committing mischief (clause 10);
- make it possible for law enforcement agencies to make a demand or obtain a court order for the preservation of electronic evidence (clause 13);
- creating new judicial production orders for obtaining data relating to the transmission of communications or data for tracking a thing or individual (clause 13);
- create warrants for obtaining transmission data in real time and for the remote activation of tracking devices in certain types of technologies (clause 17);
- modernize the deceptive marketing practices offences in the *Competition Act* (clauses 24 to 26); 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 32).

Some provisions of the bill came out of public consultations on lawful access held by representatives of Justice Canada, Industry Canada and the Solicitor General of Canada in 2002;[4] these include, specifically, the provisions relating to preservation and production.

1.3 *Convention on Cybercrime*

Canada signed the Council of Europe's *Convention on Cybercrime* in November 2001, and the Additional Protocol on hate propaganda in July 2005. The Convention criminalizes certain offences committed using computer systems, and it provides for legal tools that are adapted to new technologies, such as preservation and production orders.[5]

The Convention also provides for an order to produce data concerning subscribers[6] that is similar in some ways to a request to provide subscriber information as set out in Bill C-52,[7] which was introduced at the same time as Bill C-51. Together, bills C-51 and C-52 will mean that Canada is able to ratify the *Convention on Cybercrime* and the Additional Protocol to the Convention.

2 DESCRIPTION AND ANALYSIS

2.1 AMENDMENTS TO THE *CRIMINAL CODE*

2.1.1 MODERNIZATION OF OFFENCES

2.1.1.1 HATE PROPAGANDA (CLAUSES 4 AND 5)

Hate propaganda offences must be committed against an "identifiable group." Clause 4 of the bill adds "national origin" to the definition of "identifiable group."[8]

Clause 5 of the bill provides that the offences of public incitement of hatred and wilful promotion of hatred may be committed by any means of communication and include making hate material available, by creating a hyperlink that directs web surfers to a website where hate material is posted, for example.

2.1.1.2 DEVICE FOR THEFT OF TELECOMMUNICATION SERVICES (CLAUSE 8)

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 8 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.

2.1.1.3 COMPUTER VIRUS (CLAUSE 10)

Under the existing provisions of the Code, only spreading or attempting to spread a computer virus[9] constitutes an offence.[10] In accordance with the requirements of the *Convention on Cybercrime*,[11] Clause 10 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.

2.1.1.4 FALSE, INDECENT OR HARASSING COMMUNICATIONS (CLAUSE 11)

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.[12] Clause 11 of the bill amends those offences by removing the references to those specific communication 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 in respect of those offences 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.

2.1.2 New Investigative Tools

2.1.2.1 Preservation Demand and Order (Clause 13)

Information in electronic form may be easily and quickly destroyed or altered. Clause 13 of the bill therefore adds a new investigative tool to the Code to preserve this type of evidence, which may take one of two forms: a preservation demand or a preservation order. A preservation demand is made by a peace officer (new s. 487.012 of the Code), while a preservation order is made by a judge, on application by a peace officer (new s. 487.013 of the Code).

A preservation demand or order directs a person, such as a telecommunications service provider (TSP), to preserve "computer data"[13] that is "in their possession or control"[14] when they receive the demand or order. However, a TSP may still *voluntarily* preserve data and provide it to a law enforcement agency, even where there is no demand or order (new s. 487.0195 of the Code).

This new investigative tool is different from the data retention measure in effect in some countries,[15] which compels TSPs 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 TSP only where there are "reasonable grounds to suspect"[16] that an offence has been or will be committed[17] (new subsections 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 subsections 487.012(3) and 487.013(5) of the Code).[18]

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, and the demand may be made only once (new subsections 487.012(4) and (6) of the Code); the maximum length of a preservation order is 90 days (new subsection 487.013(6) of the Code).

A person to whom a preservation demand or order is made 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 ss. 487.0194 and 487.0199 of the Code).

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

2.1.2.2 PRODUCTION ORDERS (CLAUSE 13)

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.[19] 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.[20] Issuance of specific production orders is based on the reasonable grounds to suspect that an offence has been or will be committed.

Clause 13 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 TSP:[21] "transmission data" (new s. 487.016 of the Code) and "tracking data" (new s. 487.017 of the Code).[22]

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 does not include the content of the telecommunication.[23] This type of data is useful: for example, it may be used to identify all TSPs involved in the transmission of data and identify the initial TSP and thus determine the origin of a telecommunication (new s. 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 TSP 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 s. 487.0193 of the Code).[24] A person who has received an order may apply to a judge to revoke or vary it if production is unreasonable[25] or discloses privileged information.[26] As for a preservation order, violation of a production order is punishable by a fine of not more than $250,000 and imprisonment for a term of not more than six months, or both (new s. 487.0198 of the Code).

2.1.2.3 WARRANT FOR A TRACKING DEVICE (CLAUSE 17)

At present, section 492.1 of the Code allows a peace officer with a warrant[27] to secretly install a "tracking device"[28] (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 17 of the bill retains this type of warrant, but makes a distinction between a warrant to install a tracking device on a thing, for example a vehicle, to track its movements (new subs. 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 to track the individual's location and movements (new subsection 492.1(2) of the Code). A warrant to track the movements of a thing is based on the existing standard, 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 that kind that are found in certain types of technology, such as cellular telephones or the GPS devices in certain cars (new subsection 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 offence or organized crime offence (new subssection 492.1(5) and (6) of the Code).[29]

2.1.2.4 Warrant for a Transmission Data Recorder (Clause 17)

At present, subsection 492.2(1) of the Code allows a peace officer with a warrant[30] 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 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 17 of the bill provides for a warrant that authorizes a peace officer to install and activate a *transmission data recorder*[31] (new s. 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.

2.2 Amendments to the *Competition Act*

2.2.1 Preservation and Production Orders (Clause 20)

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 Modernization of Offences (Clauses 24 to 26)

Clauses 24 to 26 of the bill modernize certain 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.

2.3 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.[32]

2.3.1 Searches by the Commissioner of Competition (Clause 28)

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

2.3.2 Production Orders (Clause 32)

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

NOTES

1. Department of Justice Canada, "Government of Canada Introduces Legislation to Fight Crime in Today's High-Tech World," News release, 1 November 2010.
2. For more information, see Robin Mackay, *Legislative Summary of Bill C-54: Protecting Children from Sexual Predators Act*, Publication no. 40-3-C54-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 22 December 2010.
3. For more information, 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. The Legislative Summary of Bill C-52 will be available shortly.
4. See Department of Justice, Industry Canada, and Solicitor General Canada, *Lawful Access – Consultation Document*, 25 August 2002.
5. Council of Europe, *Convention on Cybercrime*, 23 November 2001, arts. 16, 17 and 19.
6. Ibid., art. 18.
7. Bill C-52: An Act regulating telecommunications facilities to support investigations, 3rd Session, 40th Parliament.

8. Under the present definition in the *Criminal Code* [the Code], subsection 318(4):

> "identifiable group" means any section of the public distinguished by colour, race, religion, ethnic origin or sexual orientation.

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

10. The Code, subsection 430(1.1). See also s. 342.2.

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

12. The Code, ss. 371 and 372.

13. The definition of "computer data" is given in subclause 9(4) of the bill. Essentially, it means data that can be processed by computer.

14. The use of the expression "in their possession or control" in the bill means that, in response to a demand or order, TSPs will probably have to retain computer data in addition to what they collect in the ordinary course of business.

15. 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.

16. 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 Code.

17. This includes an offence under the law of a foreign state.

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

19. The Code, s. 487.012 (see also new s. 487.014, introduced by the bill, which provides for a similar general production order).

20. The Code, subsections 487.013(1) and (4) (see also new s. 487.018, introduced by the bill) and subsection 492.2(2).

21. This information may also be obtained from another person who has the data in his or her possession or control, but it may not be obtained from the suspect in a police investigation.

22. See the definitions of these types of data in the Code, new s. 487.011, introduced by the bill.

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

24. A similar procedure is currently provided in s. 487.015 of the Code.

25. A recent decision of the Supreme Court of Canada shed some light on the question of whether a TSP must be reimbursed for the costs associated with executing an order to produce telephone call data. The Court held that a variety of factors should be considered, 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 TSP from which production is sought (*Tele-Mobile Co.* v. *Ontario*, [2008] 1 S.C.R. 305).

26. A production order may contain conditions to protect information covered by solicitor–client privilege (the Code, new subsection 487.019(1), introduced by the bill).

27. Where there are exigent circumstances and the conditions for obtaining a warrant exist, a warrant is not necessary. The same is true in the case of a search and the transmission date recorder (the Code, s. 487.11; see also clause 18 of the bill).

28. Under the definition in new subsection 492.1(8) of the Code, this is essentially a device that may be used to record or transmit tracking data in real time.

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

30. See s. 487.11 of the Code and clause 18 of the bill, which do not require a warrant in exigent circumstances.

31. See the definition in new subsection 492.2(6) of the Code.

32. 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*.