Legislative Summary

Bill C-29:

An Act to amend the Personal Information Protection and Electronic Documents Act

Publication No. 40-3-C29-E
23 June 2010

Alysia Davies

Legal and Legislative Affairs Division
Parliamentary Information and Research Service

Legislative Summary of Bill C-29

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-C29-E
Ottawa, Canada, Library of Parliament (2010)

CONTENTS

LEGISLATIVE SUMMARY OF BILL C-29: AN ACT TO AMEND THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

1 BACKGROUND

On 25 May 2010, the Minister of Industry introduced Bill C-29, An Act to amend the Personal Information Protection and Electronic Documents Act (short title: Safeguarding Canadians' Personal Information Act). The law that will be amended by this bill, the *Personal Information Protection and Electronic Documents Act* (PIPEDA),[1] is the main federal legislation governing privacy rights and obligations in the private sector.

PIPEDA was passed into law in 2000, and came into force in stages during the following several years. It was drafted following broad stakeholder consultations, which led to the unusual step of incorporating a voluntary industry standard (the *Model Code for the Protection of Personal Information*[2]) into the text of the legislation itself.[3]

PIPEDA is also unusual in that its jurisdictional reach extends further than many federal acts, an issue that has periodically been the subject of debate and litigation.[4] PIPEDA applies primarily to the collection, use or disclosure of personal information in the course of commercial activities by a private sector organization.[5] It regulates all such activity not only at the federal level and in the territories, but also in every province, unless that province has passed its own legislation requiring the private sector to provide comparable protection, referred to as *substantially similar* legislation.[6]

Provinces that have passed substantially similar legislation are Quebec, Alberta and British Columbia.[7] Accordingly, in those provinces PIPEDA applies only to federal organizations or to interprovincial or international transactions, while the rest of the private sector's privacy obligations are governed by the respective provincial statutes. In addition, Ontario has passed legislation that regulates the handling of personal health information by health sector custodians in all sectors;[8] PIPEDA therefore does not govern this area in Ontario, but it does continue to govern the handling of regular personal information in the rest of the private sector in that province.

The enforcement body for organizations governed by PIPEDA is the Office of the Privacy Commissioner of Canada ("the Commissioner"). The Commissioner is an ombudsperson who can receive and investigate complaints from the public or any organization concerning violations of PIPEDA. Mediation and conciliation are generally used to resolve complaints, with the aim of achieving corrective action when necessary. The Commissioner does not have the power to issue final orders, but can summon witnesses, administer oaths and compel the production of evidence in the absence of voluntary cooperation. In certain circumstances, she or he may also take cases to the Federal Court to seek an order or other resolution of a matter.

In addition, the Commissioner has the power to audit how personal information is managed by any organization governed by the Act, make public any information about such practices if it is in the public interest, and coordinate activities of various kinds with her or his provincial counterparts, including the development of model contracts for the protection of personal information in interprovincial or international transactions. The Commissioner has a public education mandate with respect to the Act as well.

PIPEDA requires a Parliamentary review of Part 1, the portion of the statute that deals with privacy and personal information, every five years.[9] The first Parliamentary review, which contained 25 recommendations for amendments to the legislation, was completed and tabled in the House of Commons in May 2007 by the Standing Committee on Access to Information, Privacy and Ethics.[10] The government subsequently issued a response to the recommendations in the Committee's report,[11] and Bill C-29 is the implementation of that response.[12]

Bill C-29 was introduced in tandem with Bill C-28, a bill containing proposed anti-spam legislation that, if adopted, would expand the enforcement powers of the Commissioner under PIPEDA. For more information on this bill, please see legislative summary 40-3-C28-E, *Bill C-28: The Fighting Internet and Wireless Spam Act*, published by the Library of Parliament.[13]

2 DESCRIPTION AND ANALYSIS

2.1 DEFINITIONS AND APPLICATION (CLAUSES 2 TO 4)

Bill C-29 adds several new definitions to PIPEDA. It preserves the existing definition of *personal information* as "information about an identifiable individual," but removes the wording excluding the names and coordinates of employees, and creates a new definition for business contact information (clauses 2(1) and 2(3)). It also specifies that PIPEDA's provisions on personal information do not apply to business contact information (clause 4).

In addition, the bill expands the coverage of PIPEDA to the personal information of applicants for employment with federal businesses, works and undertakings, instead of just employees (clause 3).

2.2 CONSENT (CLAUSE 5)

The bill inserts a new section 6.1, clarifying that individuals' consent to collection, use or disclosure of their personal information is valid only if "it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure to which they are consenting" (clause 5).

This section aims to ensure that the privacy policies and notification practices of organizations covered by PIPEDA are clear and direct in informing individuals about the ramifications of sharing personal information with these organizations, and do not try to force or mislead individuals into giving such information to the organizations.

2.3 Exceptions to Consent Requirements (Clauses 6 to 8)

However, the bill also expands the number of circumstances in which personal information can be collected, used or disclosed without consent. One new circumstance is if the personal information is contained in a witness statement and is needed to assess, process or settle an insurance claim. Another new circumstance is if the personal information was produced by the individual in the course of his/her employment, business or profession, and the collection, use or disclosure is "consistent" with the purposes for which it was produced (clauses 6(2), 6(4), and 6(10)).

As well, there are many additional new circumstances in which personal information can be disclosed without consent, including personal information requested in order to communicate with the next of kin or authorized representative of an injured, ill or deceased individual (clause 6(6)).

Another new exception is disclosure without consent when the personal information is requested to perform policing services. It should be noted that the existing exceptional circumstances in which information can be disclosed without consent under PIPEDA upon request (and under lawful authority) already include national security, defence and international affairs; enforcement of any laws of Canada, a province or a foreign country; intelligence-gathering related to enforcement of any laws of Canada, a province or a foreign country; and administration of any laws of Canada or a province. This new exception for policing services appears to add an open-ended and undefined circumstance related to law enforcement to this list. The term *policing service*s is not defined in either the Act or the bill (clause 6(6)).

The bill also re-defines the concept of *lawful authority*, which currently limits the collection, use and disclosure of personal information without consent by law enforcement authorities. The bill specifies that lawful authority is not limited to a subpoena or warrant from a court or to rules of court related to the production of records; this authority appears to be a more general authority that is left undefined. Bill C-29 also specifies that the organization disclosing the information to authorities without consent is under no legal obligation to verify that it possesses the necessary lawful authority before disclosing the information requested (clause 6(12)).

The bill expands another existing exception in the law. Subsection 7(3) of PIPEDA already permits organizations to voluntarily disclose to a government institution personal information without consent when an organization has reasonable grounds to believe that a contravention of the laws of Canada, a province or a foreign country is being, has been, or is about to be committed. Bill C-29 would allow disclosure without consent to organizations in general, presumably including other companies, if necessary to investigate a breach of an agreement or a contravention of laws (as above), or to "prevent, detect or suppress" fraud. In the case of fraud, the bill further permits disclosure without consent of an individual's personal information when notifying the individual could be reasonably expected to frustrate attempts to deal with fraud (clause 6(9)).

Another new provision would allow disclosure without consent to a government institution or to the individual's next of kin or authorized representative if there are reasonable grounds to believe that individual has been the victim of "financial abuse," and the disclosure is solely for the purpose of preventing or investigating it (clause 6(9)).

The bill therefore expands the number and type of organizations that could receive disclosures for which consent has not been obtained; this activity would no longer be limited to government actors or "investigative bodies" that currently receive such information under PIPEDA. (The bill in fact eliminates previous wording about "investigative bodies" from the Act.)

In addition, organizations may be restricted from informing individuals that their personal information has been shared if cases involve subpoenas, warrants or court-ordered production of the information; if a government institution requests the information under the national security, law enforcement or policing services exemptions; if a disclosure is made under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*; or if a disclosure is made to prevent a breach of the law. If an organization wants to notify the individual that his or her personal information has been shared under these circumstances, it must first notify the relevant authority (or other organization) that sought the personal information, which is entitled to respond within 30 days with any objections.[14] If the authority objects, the organization cannot notify the individual or disclose that the notice and objection process with the relevant authority even took place. However, the organization that shared the personal information does have to notify the Commissioner of what has occurred (clause 8).

In these cases, an organization is also prohibited from disclosing any information about what was in the subpoena, warrant or government request, and from giving the individual whose personal information is concerned access to such details (clause 8).

This particular amendment appears to create a provision similar to those in the *USA PATRIOT Act* that restrict the circumstances in which individuals may be informed that the government has requested or disclosed their personal information.[15]

The bill also changes the consent requirements for the personal information of employees of federal works, undertakings or businesses. Employers will now be able to collect, use and disclose employee information without consent if it is needed to "establish, manage or terminate" employment, provided the employee in question has been notified why the information is being collected, used or disclosed (clause 7).

The bill also adds a new ability to use and disclose personal information without the individual's knowledge or consent for the purpose of a "prospective business transaction." This exception appears to be designed to cover mergers or takeovers between companies with large holdings of personal information. Under the exception, the use or disclosure of the personal information must be necessary to determine whether to proceed with the transaction, and to then complete it. In addition, the organizations must have an agreement that requires the receiver of the personal

information to use and disclose it only for purposes related to the transaction, to protect it with appropriate security safeguards for its level of sensitivity, and to return or destroy it within a reasonable time if the transaction does not proceed (clause 7).

If the transaction does proceed and is completed, the organizations that have exchanged the personal information may use and disclose it without the knowledge or consent of the individuals involved, if the personal information is needed to carry on the business or activity that was the object of the transaction, under an agreement that it must be used and disclosed solely for the original reasons it was collected. That agreement must also again provide security safeguards at an appropriate level, and it must also stipulate that any withdrawal of consent by the individuals involved will be honoured (clause 7).

Within a reasonable time after the transaction is completed, the individuals affected must be notified of the transaction's completion and of the disclosure of their personal information (clause 7).

The bill further stipulates that all agreements under this clause between organizations exchanging personal information are binding under the law (clause 7).

However, this type of exchange without knowledge or consent may *not* take place at all, regardless of any agreements, if the primary purpose or result of the business transaction is to buy, sell, acquire, dispose of or lease personal information (clause 7).

2.4 Breach Notification (Clauses 11 to 14, 16 and 18)

Some new sections are added to PIPEDA introducing requirements to notify people when there has been a breach of the security surrounding their personal information. In particular, a new section 10.1 requires organizations to notify the Commissioner when there has been a "material breach" of the security surrounding their holdings of personal information. A new section 10.2 requires the organization to notify the individuals involved as well — unless there is any other law that prohibits it — if it is "reasonable" in the circumstances to "believe that the breach creates a real risk of significant harm to the individual" (clause 11).

Definitions are provided for how the elements of this test are met. An open-ended definition of "significant harm" is incorporated into PIPEDA, which "includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property." The key factors for identifying whether there is a real risk of significant harm are also spelled out in the Act; they are the "sensitivity of the personal information" involved and "the probability that the personal information has been, is being or will be misused"(clause 11).

There are also requirements for what the notification must contain: "sufficient information" to allow the individual to understand the significance of the breach and to take steps to mitigate or reduce harm to himself or herself from it. Any other

"prescribed information" that could be required under regulations in the future must be included as well. The notification must be "conspicuous" and given directly to the individual, provided it is feasible to do so. The notification must be provided "as soon as feasible" after a breach has been confirmed and the test for notification has been applied (clauses 11 and 18(2)).

Any government institution that could assist the individual in reducing the risk or mitigating harm from the breach must also be notified, and can make limited disclosure of the personal information without the individual's consent for the purpose of reducing the risk or mitigating the harm (clause 11).

The Commissioner is given oversight over all complaints relating to the new breach notification requirements. The requirements concerning notification of the individuals affected, and the disclosure of their personal information without consent by helpful government institutions, can also be enforced by a court order (clauses 12, 13 and 14). The Commissioner also has a mandate to encourage organizations to develop policies and practices to enforce the new requirements (clause 16).

The bill expands the list of subjects on which regulations can be made and adds a new subsection that allows the regulations to incorporate by reference any standards or specifications produced by a government or other organization. This appears to acknowledge that standards like the *Model Code* that remains part of PIPEDA's Schedule may continue to be updated as technologies and other considerations evolve (clause 18(3)).

2.5 Other Provisions

Various other clauses of the bill contain technical amendments to clarify, update or correct existing wording in PIPEDA (clauses 2(2), 9, 10(1), (2), (3), (4) and (5), 15(1) and (2), 17, 19, and 20).

Finally, the bill contains a "coordinating amendments" clause that depends on the passage of Bill C-28, the proposed anti-spam legislation introduced at the same time as this bill. It simply contains technical amendments to update the numbering of various sections in PIPEDA accordingly (clause 21).

3 COMING INTO FORCE

The bill comes into force on a day or days to be fixed by the Governor in Council (clause 22).

NOTES

1. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [PIPEDA].
2. Canadian Standards Association, *Model Code for the Protection of Personal Privacy*, CAN/CSA-Q830-96, Mississauga, Ont., March 1996.

3. The standard is in Schedule 1 of the statute and is referenced in its main provisions as well.

4. The Attorney General of Quebec launched a constitutional challenge to PIPEDA in December 2003, claiming it encroaches on provincial jurisdiction. There is also currently a constitutional challenge to PIPEDA in the Federal Court (Dockets 09-T-12, T-604-09, T-1189-09, T-1188-09, and T-1187-09) brought by a private sector organization, State Farm Mutual Automobile Insurance Company, which is challenging the federal government's jurisdiction to legislate in this area.

5. It is also intended to apply to employee information collected by employers in federal works, undertakings, or businesses, although the scope of this application is still somewhat unclear in the case law. Part 2 of PIPEDA deals with electronic documents and is primarily focused on granting them the force of legal documents as well as specifying when they are equivalent to paper copies.

6. For more information on how provincial legislation is designated substantially similar to PIPEDA, please see: Office of the Privacy Commissioner of Canada, "Substantially Similar Provincial Legislation," *Legal information related to PIPEDA.*

7. Those statutes in the three provinces are: *An Act respecting the protection of personal information in the private sector,* R.S.Q., c. P-39.1 (Quebec); *Personal Information Protection Act*, S.A. 2003, c. P-6.5 (Alberta); *Personal Information Protection Act*, S.B.C. 2003, c. 63 (British Columbia).

8. *Personal Health Information Protection Act, 2004,* S.O. 2004, c. 3, Schedule A (Ontario).

9. PIPEDA, s. 29.

10. House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA): Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics*, 1st Session, 39th Parliament, May 2007.

11. Government of Canada, "Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics: Statutory Review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)," 1st Session, 39th Parliament.

12. Industry Canada, "Backgrounder: Government of Canada Introduces Amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA)," *Government of Canada Moves to Enhance Safety and Security in the Online Marketplace*, 25 May 2010.

13. Alysia Davies, *Legislative Summary of Bill C-28: The Fighting Internet and Wireless Spam Act*, Publication no. 40-3-C28-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 28 May 2010.

14. The grounds for objection are limited to the national security exemptions; the detection, prevention or deterrence of money laundering or of financing of terrorist activities; and/or the law enforcement exemption.

15. United States, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT)*, Public Law 107-56, 107th Congress, 115 Stat. 272, 12 October 2001.