LIBRARY of PARLIAMENT
BIBLIOTHÈQUE du PARLEMENT

LEGISLATIVE SUMMARY

Bill S-4: An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act

Publication No. 41-2-S4-E
11 June 2014

Dara Lithwick

Legal and Social Affairs Division
Parliamentary Information and Research Service

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**.

Legislative Summary of Bill S-4
(Legislative Summary)

Publication No. 41-2-S4-E

Ce document est également publié en français.

CONTENTS

LEGISLATIVE SUMMARY OF BILL S-4: : AN ACT TO AMEND THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT AND TO MAKE A CONSEQUENTIAL AMENDMENT TO ANOTHER ACT

1 BACKGROUND

Bill S-4, An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act (short title: Digital Privacy Act) was introduced in the Senate and received first reading on 8 April 2014.[1]

Bill S-4 amends the *Personal Information Protection and Electronic Documents Act*,[2] the federal private sector privacy law. It does this in several notable ways, including by:

- permitting the disclosure of an individual's personal information without their knowledge or consent in certain circumstances;
- requiring organizations to take various measures in cases of data security breaches;
- creating offences for failure to comply with obligations related to data security breaches; and
- enabling the Privacy Commissioner, in certain circumstances, to enter into compliance agreements with organizations.

Following second reading in the Senate, Bill S-4 was referred to the Senate Standing Committee on Transport and Communications on 8 May 2014. The committee presented its report, containing one amendment to the bill, to the Senate on 10 June 2014 (see section 2.4.1 of this Legislative Summary).

1.1 ABOUT THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT*

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) came into being following broad consultations. In an example of multiple stakeholder cooperation, a committee of consumer, business, government, labour and professional representatives developed a set of data privacy protection principles that, in 1996, were approved as a national standard by the Standards Council of Canada. These principles were titled the *Model Code for the Protection of Personal Information*.[3] Consultations and discussion papers followed that argued for the implementation of these principles through legislation. International developments regarding data protection, particularly those taking place in the European Union, served as further impetus for the adoption of private sector privacy legislation in Canada.[4]

PIPEDA was passed into law in 2000 and came into force in three stages between 2001 and 2004.[5] PIPEDA applies primarily to the collection, use or disclosure of personal information in the course of commercial activities by a private sector organization and by federal works, undertakings and businesses. 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.") To date, Quebec, British Columbia, Alberta and, in matters relating to health care, Ontario, New Brunswick, and Newfoundland and Labrador have passed legislation deemed substantially similar to PIPEDA.[6]

Part 1 of PIPEDA addresses the protection of personal information in the private sector.[7] The purpose of PIPEDA, as set out in section 3, recognizes the relationship between the need to protect personal information and the need to use it in a world increasingly driven by information technology:

> The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[8]

Building on the work conducted by stakeholders in drafting the *Model Code for the Protection of Personal Information*, PIPEDA incorporates the Model Code into the legislation by requiring organizations subject to the Act to comply with the obligations set out in it. The Model Code is included in Schedule 1 of the Act.[9]

PIPEDA is enforced by the Privacy Commissioner of Canada, who can receive and investigate complaints from the public or any organization concerning violations of the Act.[10] The Commissioner generally uses mediation and conciliation to resolve complaints. While the Commissioner does not have the power to issue final orders to organizations, he can summon witnesses, administer oaths and compel the production of evidence if cooperation is not forthcoming. In cases that remain unresolved, the Commissioner may seek a court order from the Federal Court to achieve resolution.[11]

In addition, the Commissioner has the power to audit how personal information is managed by any organization governed by PIPEDA, make public any information about such practices if it is in the public interest,[12] and coordinate various activities with his provincial counterparts, including the development of model contracts for the protection of personal information in interprovincial or international transactions.[13] The Commissioner has a public education mandate with respect to the Act as well.[14]

1.2 Parliamentary Review of the *Personal Information Protection and Electronic Documents Act* and Efforts at Legislative Reform

PIPEDA requires a parliamentary review every five years of Part 1, the portion of the statute that deals with privacy and personal information. The first parliamentary review, which contained 25 recommendations for amendments to the legislation, was tabled in the House of Commons in May 2007 by the House of Commons Standing

Committee on Access to Information, Privacy and Ethics.[15] The government subsequently issued a response to the recommendations in the committee's report in October 2007.[16]

In May 2010, the Minister of Industry introduced Bill C-29, An Act to amend the Personal Information Protection and Electronic Documents Act.[17] Bill C-29 would have added new exceptions to consent requirements, specified what constitutes "valid consent" and imposed mandatory breach notification obligations. Bill C-29 died on the *Order Paper* with the dissolution of the 40th Parliament (26 March 2011). On 29 September 2011, the government reintroduced the bill in the 41st Parliament as Bill C-12.[18] The bill was not debated in the House of Commons prior to prorogation on 13 September 2013, when it fell from the *Order Paper*.

In addition to the government bills to reform PIPEDA, during the 1st Session of the 41st Parliament, Charmaine Borg, Member of Parliament for Terrebonne–Blainville, introduced Bill C-475, An Act to amend the Personal Information Protection and Electronic Documents Act (order-making power). This private member's bill to amend PIPEDA would have also imposed breach notification obligations and would have given the Privacy Commissioner the power to make compliance orders.[19]

In 2012, the House of Commons Standing Committee on Access to Information, Privacy and Ethics conducted a study on privacy and social media. In the course of that study, it "heard wide-ranging evidence regarding Canada's legislative framework and, more particularly, PIPEDA." The study further noted:

> While the present study's focus is on social media and privacy – and not on a legislative review of PIPEDA – this evidence should serve as an important basis upon which to inform any future discussion with respect to reviewing or modifying PIPEDA.[20]

While no subsequent statutory review of PIPEDA has taken place,[21] on 23 May 2013, the Office of the Privacy Commissioner set out its positions on PIPEDA reform in a paper entitled *The Case for Reforming the Personal Information Protection and Electronic Documents Act*.[22]

In this document, then Privacy Commissioner Jennifer Stoddart recommended:

- the Office of the Privacy Commissioner be given stronger enforcement powers;[23]
- organizations be required to report breaches of personal information to the Office of the Privacy Commissioner and to notify affected individuals where warranted;
- public reporting requirements be added to increase transparency on the use of an exception in PIPEDA that allows enforcement agencies and government institutions to obtain personal information from organizations without consent for various purposes, including national security and law enforcement; and
- PIPEDA be amended to enable the Commissioner to enter into "enforceable agreements" with organizations to ensure that they are meeting their commitments to comply with the Commissioner's recommendations following investigations.

Bill S-4 incorporates a number of the provisions found in its predecessor, Bill C-12. As well, it seems consistent with some of the recommendations made by witnesses during the 2012 privacy and social media study conducted by the committee, and by former Privacy Commissioner Stoddart in her May 2013 position paper.

2 DESCRIPTION AND ANALYSIS

2.1 DEFINITIONS AND APPLICATION (CLAUSES 2 TO 4)

Bill S-4 adds several new definitions to section 2 of PIPEDA. It preserves the existing definition of personal information as "information about an identifiable individual" but removes the wording excluding the business contact information of employees (name, title, address, telephone number). Instead, it creates a new definition for business contact information (clauses 2(1) and 2(3)). Bill S-4 also specifies that PIPEDA's provisions on personal information do not apply to business contact information (clause 4, which creates new section 4.01).

As well, new definitions are provided for "breach of security safeguards" in relation to new provisions created by clause 10, discussed later in this paper, and for "business transaction" in relation to new exceptions created by clause 7, also discussed later here (clause 2(3)).

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

Clauses 2 through 4, with minor wording differences in some of the definitions, are the same as those found in Bill C-12.

2.2 CONSENT (CLAUSE 5)

Clause 5 of Bill S-4 adds new section 6.1, clarifying that an individual's consent to the collection, use or disclosure of his or her personal information is valid only "if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting." This clause is similar to one found in Bill C-12, though the proposed provision in Bill C-12 did not specify an individual "to whom the organization's activities are directed."

This section aims to ensure that the privacy policies and notification practices of organizations covered by PIPEDA clearly and directly inform individuals about the ramifications of sharing personal information with these organizations. This section also endeavours to make sure that these policies and practices do not try to force or mislead individuals into giving such information to the organizations.

2.3 Exceptions to Consent Requirements (Clauses 6 and 7)

While clause 5 of Bill S-4 clarifies what it means to provide valid consent, clauses 6 and 7 add to the exceptions in which personal information can be collected, used or disclosed without consent.

2.3.1 Insurance and Employment

First, a new exception is added for personal information contained in a witness statement and whose collection, use or disclosure is necessary to assess, process or settle an insurance claim. Second, an exception is added for personal information produced in the course of an individual's employment, business or profession when the collection, use or disclosure is "consistent" with the purposes for which the information was produced (clauses 6(3), 6(5) and 6(11), which add new sections 7(1)(*b.1*), 7(1)(*b.2*), 7(2)(*b.1*), 7(2)(*b.2*), 7(3)(*e.1*) and 7(3)(*e.2*)). The same provisions were found in Bill C-12.

2.3.2 Communicating About an Injured, Ill or Deceased Individual

Under Bill S-4, there are new circumstances in which personal information may be disclosed without consent. Such disclosure is allowed when requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual (clause 6(7), which adds new section 7(3)(*c.1*)(iv)) or in order to identify the individual who was injured, ill or deceased. However, if the individual is alive, the organization must inform the individual without delay in writing of the disclosure (clause 6(10), which adds new section 7(3)(*d.4*)). These elements were also found in Bill C-12.[24]

2.3.3 Breaches of Agreements or Laws, Fraud and Financial Abuse

Clause 6(10) allows disclosure without consent to another organization – for example, from one business to another – in order to investigate a breach of an agreement or a contravention (or anticipated contravention) of a federal or provincial law where it is reasonable to expect that obtaining the consent from the individual for the disclosure would compromise the investigation (new section 7(3)(*d.1*)).

Furthermore, a similar disclosure provision is provided for the purposes of detecting or suppressing fraud (new section 7(3)(*d.2*)). Finally, new section 7(3)(*d.3*) allows 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 the individual has been the victim of "financial abuse," and where it is reasonable to expect that obtaining the consent from the individual for the disclosure would compromise the ability to prevent or investigate the abuse.

Clause 6(10) is similar to clause 6(9) of Bill C-12, although Bill C-12 did not contain the requirement that disclosure to the individual involved would risk compromising the investigation or ability to prevent, detect or suppress the fraud or financial abuse. As well, in Bill S-4 the threshold for the disclosure of personal information between organizations ("reasonable") differs from that in Bill C-12 ("necessary").

2.3.4 Business Transactions and Employee Information (Clause 7)

Clause 7 of Bill S-4 allows organizations to share personal information without an individual's consent for the purpose of engaging in a due diligence process for a "prospective business transaction" where such information is necessary to determine whether to proceed with the transaction or to complete it.

The organization that receives the personal information must:

- use and disclose it solely for purposes related to the transaction;
- protect it with appropriate security safeguards; and
- return the information or destroy it within a reasonable time if the transaction does not proceed (new section 7.2(1)).

Once a business transaction is completed, the organizations that have exchanged 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 provide appropriate security safeguards, and must stipulate that the organizations will honour any withdrawal of consent by the individuals involved. Furthermore, the individuals affected must be notified of the transaction's completion and of the disclosure of their personal information within a reasonable time after the transaction is completed (new section 7.2(2)).

All agreements under this clause between organizations exchanging personal information are binding under the law (new section 7.2(3)).

However, the exchange of personal information 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 (new section 7.2(4)).

Clause 7 also modifies the consent requirements for the collection, use and disclosure of the personal information of employees of federal works, undertakings and 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 or may be collected, used or disclosed (new section 7.3).

The provisions of clause 7 of Bill S-4 are the same as those found in Bill C-12.

2.3.5 Exceptions to Consent Requirements in Bill C-12 that Were Not Included in Bill S-4

Two sets of provisions in Bill C-12 relating to exceptions to consent requirements were not carried over to Bill S-4.

First, Bill S-4 does not contain a provision that redefines the concept of "lawful authority" to limit the collection, use and disclosure of personal information without consent by law enforcement authorities.[25] The absence of such a provision could be due to other legislative developments, as posited in an April 2014 blog post by Tim Banks, a partner and the Canadian lead in the global privacy and data security practice at international law firm Dentons. Banks noted:

> No doubt the government feels the pending proposed amendments to the *Criminal Code* granting organizations immunity from voluntarily collecting and disclosing information is sufficient to overcome any lingering doubts of organizations regarding the parameters for responding to pre-warrant requests for information.[26]

Second, Bill S-4 does not contain provisions that restrict the ability of organizations to inform individuals that their personal information has been shared with law enforcement and other government institutions in cases, for example, involving subpoenas, warrants or court orders for production, or if a government institution requests the information under one of the existing exemptions found in PIPEDA for national security, law enforcement or policing services (even without a court order).[27]

2.4 Breaches of Security Safeguards (Clause 10)

Clause 10 of Bill S-4 creates Division 1.1 of PIPEDA, addressing "breaches of security safeguards" and containing new sections 10.1 through 10.3 of the Act. While Bill C-12 also introduced requirements to notify people when there had been a breach of security surrounding their personal information, Bill S-4 takes a different approach.

2.4.1 Test for Breach Reporting: "Real Risk of Significant Harm"

First, clause 10 of Bill S-4, at new section 10.1 of the Act, incorporates a different test for breach reporting than that proposed in Bill C-12.

As noted by Tim Banks:

> The test for reporting a breach of security safeguards to the Office of the Privacy Commissioner in Canada in Bill C-12 involved an analysis of whether the breach was "material" having regard to a non-exhaustive list of factors.[28]

In Bill S-4, though, the proposed test emulates that found in Alberta's *Personal Information Protection Act*, the only legislation in Canada currently containing breach notification provisions.[29] In Bill S-4, an organization must report a breach to the Commissioner and notify individuals if it is "reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual."

Otherwise, the definition of "significant harm" in Bill S-4 is the same as that in Bill C-12. It is an open-ended definition that:

> 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 (new section 10.1(7)).

The factors for identifying whether there is a real risk of significant harm in Bill S-4 are the same as those in Bill C-12 ("the sensitivity of the personal information involved in the breach" and "the probability that the personal information has been, is being or will be misused"), though S-4 also includes the possibility of adding "any other prescribed factor" (new section 10.1(8)).

Finally, the contents, form and timeline for issuing a notification in Bill S-4 are mostly similar to those in Bill C-12:

- The notification must contain "sufficient information" to allow an individual to understand the significance of the breach and to take steps to mitigate or reduce any harm to him or herself that could result from it. Any other "prescribed information" that could be required under regulations in the future must be included, too (new section 10.1(4)).
- The notification must be "conspicuous" and given directly to the individual, provided it is feasible to do so (new section 10.1(5)).
- The notification must be provided "as soon as feasible" after a breach has occurred. However, if a government institution requests that the organization delay notification for a criminal investigation relating to the breach, then the notification shall not be given until the organization is authorized to do so (new section 10.1(6)).This latter element, which was not found in Bill C-12, was removed by the Senate Standing Committee on Transport and Communications in clause-by-clause review of Bill S-4.[30]

Of note, Bill C-475, which also would have created a system of mandatory breach reporting, incorporated a different threshold to report a breach to the Privacy Commissioner and to individuals affected by the breach. In Bill C-475, an organization would have to notify the Commissioner of any incident involving the loss or disclosure of, or unauthorized access to, personal information "where a reasonable person would conclude that there exists a possible risk of harm to an individual as a result of the loss or disclosure or unauthorized access." The organization would then have to notify individuals impacted by the breach if the breach "is likely to result in an appreciable risk of harm to the affected individuals."[31]

2.4.2 Notifications About Breaches to Other Organizations or Government Institutions

New section 10.2 states that an organization that notifies an individual of a breach must also notify any other organization or government institution that can reduce the risk or mitigate the harm from the breach. An organization can also make limited disclosure of the personal information to such an organization or government

institution without the individual's consent in order to reduce the risk or mitigate the harm resulting from the breach. These elements were also found in Bill C-12.

2.4.3 Records of Breaches

New section 10.3 contains an element not found in Bill C-12 requiring organizations to keep and maintain records of every breach of security safeguards involving personal information under their control. These records must be provided to the Privacy Commissioner on request.

2.5 Remedies (Clauses 11 to 15)

Clauses 11 and 12 contain consequential amendments to PIPEDA regarding compliance agreements. Clause 11 adds to section 11 of the Act – the provision on the filing of complaints – a reference to new Division 1.1, and clause 12 adds to section 12 of the Act – which deals with the investigation of complaints – a reference to new section 17.1.

Clause 13 amends section 14 of PIPEDA regarding when an applicant can apply to the Federal Court for a hearing after receiving the Commissioner's report (if still unsatisfied) or being notified that the investigation of a complaint has been discontinued. Of note, clause 13 extends the time frame from 45 days to one year for a complainant to make an application to the Court after a report or notification is sent.[32] This provision was not found in Bill C-12.

2.5.1 Compliance Agreements (Clause 15)

Clause 15, which adds new sections 17.1 and 17.2 to PIPEDA, grants the Privacy Commissioner additional powers to enter into enforceable compliance agreements with organizations that the Commissioner believes on reasonable grounds have contravened or are likely to contravene the provisions of Division 1 or 1.1, or have failed to follow a recommendation as set out in Schedule 1 of the Act (new section 17.1(1)).

The compliance agreement may contain any terms that the Commissioner considers necessary to ensure compliance with PIPEDA (new section 17.1(2)).

If an organization conforms with a compliance agreement entered into with the Commissioner, the Commissioner cannot then apply to the Federal Court for a hearing on the matter (at new section 17.1(3)). However, a compliance agreement does not stop an individual from applying to the Federal Court for a hearing or the prosecution of an offence under the Act (new section 17.1(4)).

However, if the Commissioner believes that the organization is not meeting the terms of a compliance agreement, the Commissioner must notify the organization and may then seek a mandatory order from the Federal Court to require the organization to comply with the terms of the agreement, in addition to any other remedies that the Court may give. Alternatively, the Commissioner may apply to the Court to reinstate proceedings that had been suspended as a result of the compliance agreement (new section 17.2(2)).

The provisions regarding compliance agreements should strengthen the ability of the Commissioner to enforce PIPEDA. Indeed, they seem to address the recommendation made by former Privacy Commissioner Jennifer Stoddart to amend PIPEDA to enable the Commissioner to enter into "enforceable agreements" with organizations to ensure that they are meeting their commitments to comply with the Commissioner's recommendations following investigations.

2.6 General (Clauses 17, 20, 21 and 24)

2.6.1 Confidentiality (Clause 17)

Clause 17 of Bill S-4 modifies section 20 of PIPEDA regarding what may be disclosed by the Commissioner. With some exceptions, the Commissioner is not to disclose any information that comes to his knowledge as part of the performance of his duties (section 20(1)), or contained in a breach notification report or record of a breach created by an organization (section 20(1.1)).

The other exceptions allowing for disclosure in section 20 are as follows:

- The Commissioner may make public any information that has come to his knowledge that the Commissioner considers to be in the public interest (in the exercise of his duties or powers) (section 20(2)).
- The Commissioner may disclose information necessary to conduct an investigation or audit or establish the grounds for findings and recommendations contained in any report (section 20(3)).
- The Commissioner may disclose information in the course of proceedings (such as the prosecution of an offence or a hearing before the Federal Court) (section 20(4)).
- The Commissioner may disclose to the Attorney General of Canada, or to a provincial attorney general, information related to the commission of an offence under Canadian or provincial law (section 20(5)).
- Finally, the Commissioner may disclose to a government institution any information contained in a breach notification report or an organization's record of a security breach if the Commissioner has reasonable grounds to believe that the information could be useful in the investigation of a contravention of Canadian or provincial law (section 20(6)).

2.6.2 Annual Report to Parliament (Clause 20)

Clause 20 of Bill S-4 modifies section 25 of PIPEDA to specify that the Commissioner's annual report to Parliament concerning PIPEDA must be submitted to Parliament within three months after the end of each financial year. Currently, there is no firm deadline.

2.6.3 Regulations (Clause 21)

Clause 21 of Bill S-4 broadens the regulatory powers in section 26 of PIPEDA by enabling the Governor in Council to make regulations "for carrying out the purposes and provisions of this Part" and adding the word "including" to indicate that the examples of regulation-making powers in section 26 are not exhaustive but rather open-ended. Clause 21 also adds that regulations can be made "prescribing anything that by this Part is to be prescribed." The broader regulatory powers will provide the government with more flexibility to clarify issues that might arise under PIPEDA.

2.6.4 Offence and Punishment (Clause 24)

Clause 24 of Bill S-4 modifies section 28 of PIPEDA to provide that every organization that knowingly contravenes the new sections of PIPEDA requiring organizations to record and report breaches of security safeguards or obstructs the Commissioner in the investigation of a complaint or in conducting an audit will now be liable for fines of up to $100,000 for indictable offences, or for fines of up to $10,000 for offences punishable on summary conviction.

2.7 Coordinating Amendments and Coming into Force (Clauses 26 and 27)

Clause 26 of Bill S-4 provides for coordinating amendments with the coming into force and other provisions of the new Canadian anti-spam law, *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act.*[33] As noted on the federal government's anti-spam website, the law will enter into force on 1 July 2014, except for the sections of it related to the unsolicited installation of computer programs or software, which will come into force on 15 January 2015.[34]

Clause 27 of Bill S-4 provides that clauses 10, 11, 14, 17(1), 17(4), 19 and 22 through 25 will come into force on a day to be fixed by order of the Governor in Council. The provisions in Bill S-4 that are not addressed by either clause 26 or 27 will, by default, come into force on the date on which the bill receives Royal Assent.[35]

3 COMMENTARY

Initial reaction to Bill S-4 has been generally supportive of the provisions requiring the mandatory reporting of breaches of security safeguards, and the introduction of fines for failure to record and report on such breaches.[36] As well, commentary has been positive regarding the ability of the Privacy Commissioner to enter into compliance agreements with organizations, as a step towards having greater enforcement powers.

For example, in her preliminary comments on Bill S-4, former Interim Privacy Commissioner Chantal Bernier stated:

> In particular, I welcome proposals with respect to mandatory breach notification, new penalties, and provisions that will make it easier for my Office to ensure that companies carry through on commitments they have made during investigations … I am also pleased that we will have greater discretion to publicly share more information with Canadians about our investigations.[37]

The Office of the Privacy Commissioner expressed a similar sentiment in its 4 June 2014 *Submission to the Senate Standing Committee on Transport and Communications*:

> On the whole, the proposed amendments will strengthen the privacy rights of Canadians with respect to their interactions with private sector companies, improve accountability and provide incentives for organizations to comply with the law.[38]

The greatest initial concern expressed about Bill S-4 relates to the addition of new provisions allowing personal information to be collected, used and disclosed by organizations without consent. For example, University of Ottawa law professor Michael Geist expressed concern that Bill S-4 "would expand the possibility of warrantless disclosure to anyone, not just law enforcement [referring to Bill C-13]." He added:

> Unpack the legalese and you find that organizations will be permitted to disclose personal information without consent (and without a court order) to any organization that is investigating a contractual breach or possible violation of any law. This applies both [to] past breaches or violations as well as potential future violations. Moreover, the disclosure occurs in secret without the knowledge of the affected person (who therefore cannot challenge the disclosure since they are not aware it is happening).[39]

He reiterated that concern when he appeared before the Senate Standing Committee on Transport and Communications on 4 June 2014.[40]

Similar observations were made by Peter Murphy, partner at Canadian law firm Gowling Lafleur Henderson LLP. He noted that while "Bill S-4 proposes some welcome changes to [PIPEDA], [it] also raises some worrisome concerns for the privacy of individuals." Murphy commented in particular on the provisions allowing for disclosure of personal information without consent between organizations in support of investigations of breaches of laws, agreements or cases of fraud or financial abuse. He noted:

> This change would seem to permit fishing expeditions by companies seeking to sue individuals. For example, copyright holders would have grounds to freely obtain lists of internet addresses of individuals to find and sue internet downloaders. This seems to be a significant invasion of privacy if reasonable controls are not added to the proposed wording.[41]

Other witnesses before the Senate committee, including officials from the Office of the Privacy Commissioner, and representatives from the Canadian Bar Association, the Public Interest Advocacy Centre and the Marketing Research and Intelligence Association, raised similar concerns.[42]

Revelations made at the end of April 2014 regarding the extent to which telecommunications companies disclose elements of customer data to government agencies on request appear to have added to the concerns about warrantless disclosure.[43]

Commercial stakeholders, however, seem to find the new consent requirements in the bill to be the most challenging. As noted by Adam Kardash, partner at law firm Osler Hoskin and Harcourt LLP in Toronto, the consent provision might be the bill's "most significant and problematic aspect."[44] However, this issue did not receive much attention in Senate committee hearings on the bill.[45]

NOTES

1. Bill S-4: An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act, 2nd Session, 41st Parliament.
2. *Personal Information Protection and Electronic Documents Act* [PIPEDA], S.C. 2000, c. 5.
3. Miguel Bernal-Castillero, *Canada's Federal Privacy Laws*, Publication no. 2007-44-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 1 October 2013.
4. In 1998, the European Union [EU] passed a data protection directive to ensure the protection of personal information while allowing the movement of such information as necessary within the EU. The directive required all member countries to adopt or modify existing national data protection legislation in order to comply with it. Article 25 of the directive extended its reach beyond the EU by prohibiting member countries (and businesses within them) from transferring personal information to any non-member country whose laws did not sufficiently guarantee the protection of that information. See European Parliament, Council of the European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, 24 October 1995.
5. On 1 January 2001, the Act applied to the federally regulated private sector (i.e., banking, telecommunications, interprovincial transportation). On 1 January 2002, personal health information became subject to the Act and on 1 January 2004, the Act applied to the whole of the private sector, even to organizations that only collect, use or disclose information within a particular province. Organizations in the Northwest Territories, Yukon and Nunavut are considered to be federal works, undertakings or businesses under PIPEDA.
6. Office of the Privacy Commissioner of Canada, "Complying with the *Personal Information Protection and Electronic Documents Act*," *Fact Sheets*.
7. 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.

8. PIPEDA, s. 3.

9. The federal constitutional jurisdiction for PIPEDA is largely grounded in federal jurisdiction over trade and commerce, though commentators have noted that "Part 1 of PIPEDA has both federal and provincial characteristics, which is a necessary incident of its design to regulate the flow of personal information nationally and internationally." (Josh Nisker, "*PIPEDA*: A Constitutional Analysis," *The Canadian Bar Review*, Vol. 85, 2006, p. 342.)

   In December 2003, the Attorney General of Quebec launched a constitutional challenge to PIPEDA, claiming it encroaches on provincial jurisdiction. That case is ongoing but has remained largely dormant. See Michael Geist, "State Farm challenges Canada's privacy law in court," *The Toronto Star*, 5 April 2010.

   On 9 July 2010, the Federal Court restricted the scope of the definition of "commercial activity" in PIPEDA following a constitutional challenge brought by a private sector organization, State Farm Mutual Automobile Insurance Company. The company questioned whether the provisions of PIPEDA apply to evidence collected by an insurer, on behalf of an insured, in a tort action. Justice Robert Mainville determined that PIPEDA does not apply to such evidence as there is no commercial character associated with that activity, being between two individuals (PIPEDA applies to commercial activities). This decision effectively limits the application of privacy laws to information-gathering by or on behalf of individuals. See *State Farm Mutual Automobile Insurance Company v. The Privacy Commissioner of Canada*, 2010 FC 736.

10. PIPEDA, s. 11.

11. Ibid., ss. 14–17.

12. Ibid., s. 18.

13. Ibid., ss. 23 and 23.1.

14. Ibid., s. 24.

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

16. ETHI, *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),* 2nd Session, 39th Parliament, October 2007.

17. Bill C-29: An Act to amend the Personal Information Protection and Electronic Documents Act, 3rd Session, 40th Parliament.

18. Bill C-12: An Act to amend the Personal Information Protection and Electronic Documents Act, 1st Session, 41st Parliament.

19. Bill C-475: An Act to amend the Personal Information Protection and Electronic Documents Act (order-making power), 1st Session, 41st Parliament. This bill was carried over to the 2nd Session, 41st Parliament and defeated at second reading, 29 January 2014. While Bill C-475 would have also imposed mandatory breach notification obligations, it would have done so using a different standard and approach than that found in Bill C-29.

20. ETHI, *Privacy and Social Media in the Age of Big Data*, Fifth Report, 1st Session, 41st Parliament, April 2013, p. 34. A number of witnesses who appeared during the study also commented on Bill C-12.

    For example, Tamir Israel of the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic at the University of Ottawa observed that Bill C-12 "provides a workable framework for breach notification, but it requires fixes and a commitment to introduce penalties for non-compliance if it is to be effective" (p. 35).

    Jennifer Stoddart, then the Privacy Commissioner of Canada, expressed concern that "in its current form, Bill C-12 was not an adequate solution to the constant and growing threat of data leakage and data-related breaches of confidence" (p. 36). She suggested that one idea that could strengthen the legislation would be to establish a penalty system to encourage companies "to invest in data protection and act as a deterrent to breaches of confidence, while remaining flexible and adaptable so as not to unduly burden smaller organizations" (p. 36).

21. According to section 29 of PIPEDA, a statutory review would have been due in 2011–2012 (five years following the previous review).

22. Office of the Privacy Commissioner of Canada, "The Case for Reforming the *Personal Information Protection and Electronic Documents Act*," *PIPEDA Review*, 23 May 2013.

23. Options include statutory damages to be administered by the Federal Court, and providing the Privacy Commissioner with order-making powers and/or the power to impose administrative monetary penalties where circumstances warrant.

24. However, Bill C-12 included an additional provision allowing disclosure for the "purpose of performing policing services" that are not otherwise included in other parts of section 7. 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.

25. Bill C-12, c. 6(12).

26. Tim Banks, "Canada's Digital Privacy Rethink: Fines, Enforceable Compliance Agreements and More!," *Dentons Privacy and Data Security Law* (Blog), 9 April 2014. Mr. Banks is referring to Bill C-13: An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act, 2nd Session, 41st Parliament (first reading version, 20 November 2013).

    Clause 20 of Bill C-13 provides that a telecommunications service provider may voluntarily preserve data and provide it to a law enforcement agency, even where there is no preservation demand or order, without incurring any criminal or civil liability (new section 487.0195 of the *Criminal Code*). For more on Bill C-13, please consult Julia Nicol and Dominique Valiquet, *Legislative Summary of Bill C-13: An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, Publication no. 41-2-C13-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 11 December 2013.

27. Bill C-12, c. 8.

28. Banks (2014).

29. Organizations subject to the *Personal Information Protection Act*, S.A. 2003, chapter P-6.5 are required to report a breach of personal information to the Alberta Information and Privacy Commissioner as follows:

> 34.1(1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

30. See Senate, Standing Committee on Transport and Communications, *Evidence*, 2nd Session, 41st Parliament, 10 June 2014. Following witness testimony it was considered that notice to individuals should not be delayed even where there is a criminal investigation under way, as a delay could negatively impact the individuals whose personal information has been compromised by a breach of security safeguards.

31. Bill C-475, c. 1 (proposed ss. 10.01 and 10.02 of PIPEDA).

32. At the 22nd annual convention of access to information and privacy advisors of *l'Association sur l'accès et la protection de l'information*, held on 16 April 2014 in the city of Québec, Interim Privacy Commissioner Chantal Bernier commented in her opening remarks how the one-year time frame better corresponds to the amount of time that it actually takes to negotiate on an issue. See Patrick Cormier, "Protection De La Vie Privée Au Canada: Finalement, Des Dents Plus Longues!," *Slaw*, 16 April 2014.

33. *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23.

34. Government of Canada, "Fast Facts," *Canada's Anti-Spam Legislation*.

35. *Interpretation Act*, R.S.C., 1985, c. I-21, s. 5.

36. See, for example, Emily Chung, "New privacy rules target data breaches, fraud: Privacy commissioner would get new enforcement powers under Digital Privacy Act," *CBC News*, 10 April 2014.

37. Chantal Bernier, Interim Privacy Commissioner of Canada, "Statement from the Interim Privacy Commissioner of Canada regarding Bill S-4, the *Digital Privacy Act*," News release, 8 April 2014.

38. Office of the Privacy Commissioner of Canada, *Bill S-4, An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act: Submission to the Senate Standing Committee on Transport and Communications*, 4 June 2014.

39. Michael Geist, "Why the Digital Privacy Act Undermines Our Privacy: Bill S-4 Risks Widespread Warrantless Disclosure," (Blog), 10 April 2014.

40. Michael Geist, "Diving Into the Digital Privacy Act: My Appearance Before Senate Transport & Comm Committee on S-4," (Blog), 5 June 2014.

41. "Canada: PIPEDA reforms propose breach notification, CAN $100,000 fines," *Privacy This Week*, 17 April 2014.

42. Senate, Standing Committee on Transport and Communications, *Evidence*, 2nd Session, 41st Parliament, 3 June 2014 and 4 June 2014.

43. Steven Chase and Colin Freeze, "Reports of massive public surveillance badly timed for Conservatives' cyberbills," *The Globe and Mail* [Toronto], 1 May 2014.

44. Mark Burgess, "Business lobby set to take on government's Digital Privacy Act: Lobbyists are lining up in response to the government's digital privacy bill," *The Hill Times* [Ottawa], 28 April 2014.

45. One group, the Public Interest Advocacy Centre, expressed concern that the provision is redundant and could "create confusion." See Senate Standing Committee on Transport and Communications, *Evidence*, 2nd Session, 41st Parliament, 4 June 2014 (John Lawford, General Counsel and Executive Director, Public Interest Advocacy Centre).