Canada’s Federal Privacy Laws

Publication No. 2007-44-E
1 October 2013

Miguel Bernal-Castillero
Economics, Resources and International Affairs Division
Parliamentary Information and Research Service
Library of Parliament **Background Papers** provide in-depth studies of policy issues. They feature historical background, current information and references, and many anticipate the emergence of the issues they examine. 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 in an objective, impartial manner.
## CONTENTS

1 INTRODUCTION .............................................................................................................. 1

2 LEGISLATIVE HISTORY ................................................................................................. 1

3 FEDERAL PRIVACY LAWS .............................................................................................. 3

3.1 The Privacy Act ........................................................................................................... 3

3.2 Proposals for Amending the Privacy Act .................................................................. 5

3.3 The Personal Information Protection and Electronic Documents Act .................. 6

3.4 Statutory Review of the Personal Information Protection and Electronic Documents Act ................................................................. 8

4 CONCLUSION ................................................................................................................. 10

APPENDIX A – THE 10 PRIVACY PRINCIPLES FROM THE CANADIAN STANDARDS ASSOCIATION MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION
1 INTRODUCTION

Classically understood as the right to be left alone, the concept of privacy in today’s high-tech world has taken on many new dimensions. Experts in this area equate privacy with the right to enjoy private space, to conduct private communications, to be free from surveillance and to have the sanctity of one’s body respected. To most people, it is essentially about control over what is known about them and by whom.

Privacy protection laws in Canada focus mainly on safeguarding personal information. Drawing upon generally accepted fair information practices, federal data protection laws – namely, the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA) – seek to allow individuals to decide for themselves, to the greatest extent possible, with whom they will share their personal information, for what purposes and under what circumstances. Thus, what one person views as an intolerable intrusion upon privacy may be acceptable to another.

The Privacy Act governs the federal public sector. It obliges approximately 250 federal government institutions to respect the privacy rights of individuals by limiting the collection, use and disclosure of their personal information. The Privacy Act also gives individuals the right to request access to personal information about themselves held by federal government institutions. If individuals feel that the information is incorrect or incomplete, they also have the right to ask that it be corrected.

PIPEDA, for its part, sets out ground rules for the management of personal information in the private sector. It aims to strike a balance between an individual’s right to the privacy of personal information and the need of organizations to collect, use or disclose personal information for legitimate business purposes. PIPEDA applies to organizations engaged in commercial activities throughout Canada other than in provinces that have “substantially similar” private-sector privacy laws. PIPEDA also protects employee information, but only in federally regulated sectors.

This paper will provide an overview of the federal landscape with respect to privacy legislation, its legislative history, and the need for modernization at a time when technology, digitization, social media and concerns about national security and the threat of terrorism are rapidly transforming the way in which personal information is created, accessed, retained and discarded.

2 LEGISLATIVE HISTORY

Concerns about the protection of personal information first arose in Canada during the late 1960s and early 1970s when computers were emerging as important tools for government and big business. In response to a federal government task force report on privacy and computers, Canada enacted the first federal public sector privacy protection in Part IV of the Canadian Human Rights Act in 1977. This
provision established the office of the Privacy Commissioner of Canada as a member of the Canadian Human Rights Commission and provided the Privacy Commissioner with the mandate to receive complaints from the general public, conduct investigations and make recommendations to Parliament.

Arguably, the anti-discrimination provisions of the Canadian Human Rights Act were not the best fit for the right to privacy, leaving a legislative gap that was addressed by the current Privacy Act and the Access to Information Act, both of which came into force in 1983. Both pieces of legislation stemmed from the same bill (Bill C-43) and from a belief in the complementary nature of data protection and freedom of information as critical components of a strong and healthy democracy.

At the same time as Canada was addressing questions of data protection in a networked world, the European community was also responding to what it perceived as threats to the fundamental right to privacy that were being posed by the advent of networked computers that could readily be used to exchange information. As a result, various federal and state data protection laws were enacted in Europe in the 1970s, and in January 1981 the Council of Europe opened for signature the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Convention required member states to introduce data protection legislation that complied with a set of framework principles pertaining to the collection, use, access, accuracy and disposal of personal information.

On 23 September 1980, the Organisation for Economic Co-operation and Development (OECD) adopted the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data in order to harmonize the data protection practices of member countries by means of minimum standards for handling personal information. Although the OECD Guidelines are voluntary and have no force in law, they have served as the foundation for legislated fair information practices in Canada and in many other countries. The OECD Guidelines were revised in July 2013, in an effort to modernize the original 1980 version and adapt it to the new realities of privacy protection in a data-driven economy.

The vast majority of countries in the OECD have enacted data protection laws extending to both the public and private sectors. However, when Canada affirmed its commitment to the OECD Guidelines in 1984, Canadian laws, with the exception of Quebec’s private sector legislation, applied only to the actions of governments and government agencies. Although the federal government, and indeed the federal Privacy Commissioner, were content at that time to encourage the private sector to develop and adopt voluntary privacy protection codes, by the end of the 1980s the Privacy Commissioner was concerned about the lack of progress in this regard and called for federal legislation mandating federally regulated corporations to develop such codes of practice.

In response to the lack of national data protection standards in Canada, a committee of consumer, business, government, labour and professional representatives developed, under the auspices of the Canadian Standards Association (CSA), a set of privacy protection principles that in 1996 were approved as a national standard by the Standards Council of Canada. The Model Code for the Protection of Personal
Information (see Appendix A) was designed to serve as a model that could be adopted by businesses and modified to suit their particular circumstances.

At about the same time, the Minister of Industry created the Information Highway Advisory Council to advise him on how Canada could best benefit from the potential of electronic commerce. In response to a public discussion paper, most consumer representatives, privacy commissioners and advocates called for legislated privacy protection, while businesses, for the most part, preferred a self-regulatory approach pursuant to the CSA standard. Ultimately, the Advisory Council recommended to government that flexible framework legislation be developed, based on the CSA standard.

Another impetus for Canada’s move toward private sector privacy legislation was the European Union’s data protection directive, which in 1998 required all member countries to adopt or adapt national data protection laws to comply with the Union’s Directive on Data Protection. Article 25 of the Directive prohibits member countries of the European Union (and businesses within those countries) from transferring personal information to any non-member country whose laws do not adequately guarantee protection of that information.

In January 1998, an Industry Canada Task Force on Electronic Commerce released a discussion paper, *The Protection of Personal Information – Building Canada’s Information Economy and Society*, in which it was noted that ensuring consumer confidence was essential to the growth of the information economy. The authors observed that “legislation that establishes a set of common rules for the protection of personal information will help to build consumer confidence and create a level playing field [so that] the misuse of personal information cannot result in a competitive advantage.” The outcome of this consultative process was the development of a private sector legislative regime that drew on laws in other countries and that, in a rare move, incorporated the text of the CSA Model Code. Bill C-54, the Personal Information Protection and Electronic Documents Act, was introduced in the House of Commons in October 1998. The bill died on the Order Paper with the prorogation of Parliament; however, it was reintroduced under the same title as Bill C-6 in October 1999 and came into force on 1 January 2001.

Although the *Privacy Act* and PIPEDA came into force 18 years apart and are considered “first-” and “second-generation” privacy laws, respectively, they both have a principle-based approach whose basic premise is that individuals should, to the greatest extent possible, have control over what is known about them and by whom.

## 3 FEDERAL PRIVACY LAWS

### 3.1 THE PRIVACY ACT

The *Privacy Act* is a data protection law, once described as an “information handler’s code of ethics.” The law has three basic components, as follows:

- it grants individuals the legal right of access to personal information held about them by the federal government;
• it imposes fair information obligations on the federal government with regard to how it collects, maintains, uses and discloses personal information under its control; and
• it puts in place an independent ombudsman, the Privacy Commissioner, to resolve problems and oversee compliance with the legislation.

The Privacy Act applies only to the approximately 250 federal government departments and agencies set out in the Schedule to the Act.

Personal information under the Act (section 2) includes any information about an identifiable individual, recorded in any form (e.g., video or audiotape, or any electronic medium), including information about age, education, medical history, criminal record or employment history (e.g., tax records, student loan applications). The Act stipulates that no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution (section 4). As well, wherever possible, the information should be collected directly from the individual to whom it relates and the individual should be informed of the purpose for which it is being collected (section 5). In the interests of transparency and openness, government institutions are required to publish indexes indicating all of the personal information banks maintained by these institutions (sections 10 and 11).

The central privacy principle under the Act is that personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose (section 8). The Act does, however, contain a list of 13 uses and disclosures that might be permissible without the consent of the individual (e.g., national security, law enforcement, public interest).

Everyone in Canada has the right to apply for access to personal information about himself or herself that is held by the federal government (sections 12 to 17). If an individual is not satisfied with the accuracy of the information obtained, he or she may seek to have the inaccuracies corrected (section 12(2)(a)). If such a request is refused, the applicant is entitled to require that a notation be attached to the information describing any corrections requested but not made (section 12(2)(b)). The Act provides a number of exemptions that may be used by a government institution to prevent an applicant from having access to part or all of his or her personal information held by the institution (sections 18 to 28). If an applicant is not satisfied with the action of a government institution, a complaint can be made to the Privacy Commissioner (sections 29 and 30). On the basis of a complaint, the Commissioner conducts an investigation and issues his or her findings (sections 31 to 35). Where the complaint is well-founded, the Commissioner can render non-binding recommendations to the government institutions (section 35). Findings that the Commissioner considers are in the public interest are published in the Privacy Commissioner’s Annual Report to Parliament (section 37(4)). In situations where this recourse is unsuccessful, an application for judicial relief can be made to the Federal Court (sections 41 to 52).
In addition to investigating complaints about the operation of the Privacy Act, the Privacy Commissioner can conduct audits of the fair information practices of government institutions and carry out special studies referred to the Commissioner by the Minister of Justice (section 60).\textsuperscript{14}

### 3.2 PROPOSALS FOR AMENDING THE PRIVACY ACT

In June 2006, in response to an invitation from the House of Commons Standing Committee on Access to Information, Privacy and Ethics, the Privacy Commissioner of Canada, Jennifer Stoddart, presented the Committee with a comprehensive set of proposals for changes to the Privacy Act.\textsuperscript{15} The document, in which the Commissioner noted “the rapid technological changes in all aspects of government and in the activities it regulates,” identified key areas where the Privacy Act could be strengthened and modernized to further ensure that government is both responsible and fully accountable for the personal information in its control. The Commissioner later published an Addendum to the document, in which she provided additional comment in the areas of national security, transborder data flows, breach notification and legislative coverage.\textsuperscript{16} In response to these documents and the need for reform, the Access to Information, Privacy and Ethics Committee commenced a review of the Privacy Act in the spring of 2008.

In June 2009, the Committee issued a report in which it endorsed many of the Commissioner’s “quick fixes” for the Privacy Act – the most important and necessary reforms that could be easily and quickly implemented, pending a comprehensive review of the Act.\textsuperscript{17} In addition to recognizing that “a complete overhaul of the Act is in fact warranted,” the Committee made the following specific recommendations:

- the expansion of the Privacy Commissioner’s mandate to provide her Office with a clear public education mandate;
- strengthening the annual reporting requirements of government departments and agencies so that they report on a broader spectrum of privacy-related activities;
- the introduction of provisions requiring proper security safeguards for the protection of personal information; and
- the introduction of provisions for an ongoing five-year Parliamentary review of the Act.

The Committee also supported the Commissioner’s recommendation to eliminate the restriction by which the Privacy Act applies only to information collected by the federal government in “recorded” form. As the Commissioner explained, new technologies such as live feeds of surveillance footage from cameras and DNA swab information collected from individuals do not meet this now dated description.

The Committee discussed other recommendations, but noted that they required further study and consideration before being proposed as legislation. Of note among these was the creation of a “necessity test,” similar to that under PIPEDA, to ensure that departments and agencies demonstrate a need for the information they are collecting.
Another such recommendation was the broadening of the grounds for which matters can be brought before the Federal Court and of the legal remedies available. Currently, the Act allows complainants or the Privacy Commissioner the right to go to the Federal Court only in relation to the denial of access to personal information. Put another way, there is no recourse to the courts when there has arguably been an inappropriate collection, use or disclosure of personal information by government institutions. Further, the Act currently does not give the Federal Court the power to award damages against offending institutions, a situation the Commissioner and other commentators suggest should change.

Other major changes to the Privacy Act that have been proposed concern the disclosure of personal information by the Canadian government to foreign states. Currently, the Act allows the Canadian government to share personal information about its citizens with foreign governments where there is an agreement to do so and the purpose is to administer a law or conduct an investigation. Privacy advocates suggest that the Act be strengthened and point to the example of the European Union, which restricts the disclosure of government-held information to those foreign states that provide adequate levels of privacy protection.

In its response to the Committee’s Report and recommendations, the government noted its view that the Privacy Act is “a strong piece of legislation” and that “it is crucial that careful consideration be given to the impact changes to the legislation may have on the operations of government institutions which are subject to the Act.” To date, no legislation has been put forth to substantively amend the Privacy Act.

### 3.3 The Personal Information Protection and Electronic Documents Act

PIPEDA establishes rules governing the collection, use and disclosure of personal information by organizations in the private sector, but only in the course of commercial activities. Essentially, the legislation seeks to balance an individual’s right to privacy with the reasonable needs of organizations to collect, use and disclose information for economic purposes. The Act also applies to the collection, use and disclosure of personal information pertaining to the employees of federally regulated organizations. It does not apply to any government institution to which the federal Privacy Act applies, to personal information collected, used or disclosed by an individual exclusively for personal or domestic purposes, or to organizations in respect of personal information that is collected, used or disclosed for journalistic, artistic or literary purposes.

In response to concerns raised within the health sector concerning the application of the privacy protection provisions of the bill to personal health information, PIPEDA’s implementation occurred in three stages.

- On 1 January 2001, the Act covered interprovincial or international trade in personal information and applied only to the federally regulated private sector (i.e., telecommunications, broadcasting, banking, interprovincial transportation and airline industries).
- On 1 January 2002, personal health information became subject to the Act.
Since 1 January 2004, the provisions of the Act have been extended more broadly to include all organizations located entirely within a province, even if they collect, use or disclose personal information only within that province.

However, if a province has enacted legislation that has by Order of the Governor in Council been deemed to be “substantially similar” to PIPEDA, organizations covered by the provincial legislation may be exempted from the application of the federal Act. To date, only the legislation in Alberta, British Columbia and Quebec have been deemed “substantially similar” to PIPEDA. New Brunswick, Newfoundland and Labrador, and Ontario have laws that are substantially similar to PIPEDA with respect to the custodianship of health information, but even in these provinces PIPEDA continues to apply to the federally regulated private sector and to personal information in interprovincial and international transactions.

Organizations subject to PIPEDA are required to comply with the 10 privacy principles and the individual's right of access to his or her personal information set out in the Canadian Standards Association’s Model Code for the Protection of Personal Information (section 5 and Schedule 1 of the Act – see Appendix A). Essentially, organizations are responsible for the protection of personal information and the fair handling of that information at all times, both internally and in dealings with third parties. With limited exceptions, they are required to obtain an individual's consent when collecting, using or disclosing his or her personal information (section 7). Purposes for which an organization can collect, use, or disclose personal information are limited to those that “a reasonable person would consider are appropriate in the circumstances” (sections 3 and 5(3)). Personal information can be used only for the purpose for which it was collected; should an organization wish to use the information for another purpose, consent must be obtained again. Individuals must also be assured that their information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords or encryption.

Under PIPEDA, the Privacy Commissioner has the power to receive or initiate, investigate and attempt to resolve complaints about any aspect of an organization’s compliance with the law’s data protection provisions (sections 11 and 12). The Commissioner will usually attempt to resolve the matter through persuasion and negotiation; however, in cases where the ombudsman approach fails, recourse may be had to the Federal Court for judicial remedies, including orders to comply and to pay damages (sections 12.1, 14 and 16).

The Commissioner also has the following powers:

- to audit the personal information management practices of an organization (section 18);
- to make public any information relating to an organization’s personal information practices when it is in the public interest to do so (section 20);
- to enter into agreements with his or her provincial counterparts to coordinate activities (section 23);
• to undertake and publish research and develop model contracts for the protection of personal information that is collected, used or disclosed interprovincially or internationally (sections 23 and 24); and
• to develop and conduct information programs to foster public understanding of the provisions of PIPEDA (section 24).

In December 2010, Parliament passed anti-spam legislation with the aim of deterring unwanted electronic communications.21 This legislation amended PIPEDA by expanding the Privacy Commissioner’s investigative powers and permitting the Commissioner to take measures against the unauthorized collection of personal information through hacking or the illicit trading of electronic addresses.22 Once fully in force,23 the anti-spam legislation will complement PIPEDA in regulating certain online commercial practices, such as the sending of commercial electronic messages (by requiring senders to obtain prior consent), as well as the harvesting of electronic addresses and the installation of malicious software on computers. Under the legislation, the Office of the Privacy Commissioner will share enforcement responsibilities with the Canadian Radio-television and Telecommunications Commission and with the Competition Bureau.

3.4 STATUTORY REVIEW OF THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

Pursuant to section 29 of PIPEDA, a House of Commons committee or a joint committee of both Houses is required every five years to review Part 1 of the Act, Protection of Personal Information in the Private Sector.24 The first scheduled review of PIPEDA was conducted by the House of Commons Standing Committee on Access to Information, Privacy and Ethics between November 2006 and February 2007, and a report including 25 recommendations was tabled in May 2007.25

The report did not advocate major changes to the legislation. The Committee was concerned that, as the Act was not fully implemented until January 2004, not every aspect of the law could be adequately reviewed. Thus, the Committee, for the most part, limited itself to suggesting adjustments to the legislation to ensure greater harmonization between PIPEDA and substantially similar private sector data protection laws in the provinces of Quebec, Alberta and British Columbia.

By way of example, the Committee referred to the personal information protection legislation of British Columbia and Alberta in recommending that the form and adequacy of consent, the cornerstone of most data protection statutes, be clarified, distinguishing between express, implied and deemed or opt-out consent. As well, the Committee tackled the issue of whether the current consent model under PIPEDA, which was designed for commercial contexts, should be applied to the employment sector. After reviewing the approaches taken in Quebec, British Columbia and Alberta to privacy protection in the workplace, the Committee saw a need to create a separate federal employment model under PIPEDA.

With respect to law enforcement and national security issues, the Committee recommended the removal of a controversial provision that was added to PIPEDA in 2002 in response to the events of 11 September 2001. Section 7(1)(e) of PIPEDA
allows for the collection and use of personal information without the knowledge or consent of the individual involved for purposes that were previously permitted only in the case of disclosing such information (i.e., reasons of national security, the defence of Canada, the conduct of international affairs or where required by law).\textsuperscript{26} The new collection power in section 7(1)(e) troubled privacy advocates, including the federal Privacy Commissioner, who felt that the provision had the undesirable effect of requiring the private sector to carry out law enforcement activities without corresponding state accountability.

The most comprehensive Committee recommendation was made in relation to the duty of private sector organizations to notify individuals in instances of security breaches of personal information holdings. The Committee was aware of mounting public concern in this area, since major breaches involving personal information were increasingly coming to light. The Committee was also cognizant of the fact that many American states have passed laws requiring that customers be notified when their personal information has been compromised. Although the Committee did not endorse “mandatory breach notification,” it did favour a model whereby organizations would be required to report certain defined breaches to the Privacy Commissioner, who would then conduct an analysis to determine whether notification should be made and, if so, in what manner.

Finally, the Committee emphasized the need to invest more resources in educating individuals and organizations about their respective rights and responsibilities under PIPEDA. In the Committee’s view, the success of any amendments to the Act, and ultimately of the Act itself, depends on individuals being able to make informed choices about their personal information and on organizations being fully aware of their obligations under the law.

In its response to the Committee’s Report, the government agreed that no significant change were needed at this time with respect to PIPEDA, accepted most of the Committee’s 25 recommendations, and made a commitment to conduct further consultations in several areas before presenting any legislative and policy proposals for parliamentary consideration.\textsuperscript{27} On 25 May 2010, the government introduced Bill C-29, An Act to amend the Personal Information Protection and Electronic Documents Act, later reintroduced as Bill C-12 in the 41\textsuperscript{st} Parliament.\textsuperscript{28}

The proposed legislation includes several of the amendments to PIPEDA suggested by the Committee, including changes aimed at clarifying consent, making consent valid only if

\begin{quote}
\textit{it is reasonable to expect that the individual understands the nature, purpose and consequence of the collection, use or disclosure to which they are consenting.}\textsuperscript{29}
\end{quote}

Bill C-12 also seeks to change the consent requirements pertaining to the personal information of employees of federal works, undertakings or businesses, allowing employers to collect, use and disclose employee information without consent if this information is needed to “establish, manage or terminate” employment, as long as the employee has been notified that the information is being collected, used, or disclosed and why.\textsuperscript{30}
The bill creates other exceptions to consent requirements, including when the personal information is requested to perform policing services, and expands the number and type of organizations that could receive disclosures for which consent has not been obtained to go beyond government actors, law enforcement and national security agents, while limiting the situations in which individuals would need to be informed of such disclosures.  

Most significantly, Bill C-12 introduces new breach notification provisions, placing new responsibilities on organizations to report instances where the personal information they hold is subject to a security breach. Where there has been a “material breach,” an organization must notify the Privacy Commissioner of the security safeguards involving personal information under its control. In cases of a breach that creates “a real risk of significant harm to the individual,” organizations must notify the individuals of the breach as well as any government institution that could assist in reducing the risk or mitigating harm from the breach. Although the bill provides organizations with the key factors in identifying whether there is a real risk of significant harm, as well as the requirements for what the notification must contain, oversight of complaints relating to the new breach notification requirements rest with the Privacy Commissioner.

Bill C-12 has not advanced beyond first reading since its introduction in September 2011. With the prorogation of the 1st Session of the 41st Parliament on 13 September 2013, Bill C-12 has been dropped from the Order Paper, and it is uncertain whether the bill will be reintroduced in the next parliamentary session.

Commentators, including the Privacy Commissioner, have been generally welcoming of the amendments proposed in Bill C-12, noting them as a positive first step in addressing privacy-related concerns while nonetheless expressing concern that the provisions on breach notification, in particular, will require the introduction of a penalty scheme for non-compliance for them to be effective. However, the second five-year review of PIPEDA is now overdue, and concerns have arisen that Bill C-12 may already be outdated, such that the bill and PIPEDA have fallen behind the rapid advances in computing and the scale in which personal information can be collected and stored, used and disclosed.

Most recently, in May 2013, the Privacy Commissioner published a comprehensive paper arguing for an in-depth reform of PIPEDA, one that goes beyond what is currently proposed in Bill C-12. In her document, the Privacy Commissioner argues for stronger enforcements powers, mandatory breach notification, public reporting on the number of disclosures that organizations make to law enforcement, and modifications to the accountability principles in Schedule 1 of the Act.

4 CONCLUSION

As advances in technology increase the ease with which information about individuals can be gathered, stored and searched, the need to protect the privacy of such information presents a rapidly evolving challenge for legislators. Even the definition of privacy itself is open to debate. Some advocates contend that privacy is a core human and societal value that implies more than control over one’s personal
information or the right to be left alone. Others view as inevitable in the Internet age a blurring of lines between personal and public realms, along with shifting attitudes about what information we are willing to share and with whom.

Although the use of personal data presents commercial opportunities, these need to be balanced with individuals’ privacy rights. In addition, legislation to protect personal information must take into account the impact of privacy protections on law enforcement and national security. Ultimately, the extent to which legislative protections can keep pace with rapidly advancing technologies remains to be seen.

Meanwhile, the flexibility and adaptability of Canada’s federal privacy laws are being tested more than ever before. No matter how the right to privacy is ultimately defined or safeguarded in this country, emerging privacy issues will continue to challenge legislators, businesses and industries, and individuals.

NOTES

† An earlier version of this document, dated 25 September 2008, was prepared by Nancy Holmes of the Library of Parliament.


7. OECD, OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, revised 11 July 2013. The new 2013 OECD Privacy Guidelines introduce several new concepts, including security breach notification, privacy management programs, national privacy strategies, education and awareness, and global interoperability. Other revisions expand or update existing provisions, such as those related to the accountability of data controllers, transborder data flows, privacy enforcement and international cooperation. It is worth noting that the “eight basic principles of national application,” which are contained in Schedule 1 of PIPEDA, have been left intact from the original 1980 OECD Privacy Guidelines.

8. Quebec’s Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q. c. P-39.1, which came into force in 1994, applies the fair information principles of the OECD Guidelines to all personal information, whatever its form and in whatever medium that it is collected, held, used or distributed by any private sector organization (i.e., not just with respect to commercial activities).


12. The Privacy Commissioner is an Officer of Parliament who is appointed by the Governor in Council for a maximum of seven years. For more details, see the Office of the Privacy Commissioner of Canada [OPC] website.

13. Summaries of findings under the *Privacy Act* are available at OPC, *Findings under the Privacy Act*.


19. PIPEDA is limited in its scope to commercial activities because the provinces have exclusive jurisdiction over matters of private property and civil rights. The federal government therefore chose to regulate this area on the basis of its general power to regulate trade and commerce. However, according to a constitutional challenge filed by the Quebec government in 2003, the federal government has exceeded its jurisdiction under PIPEDA in that it interferes with Quebec’s constitutional competence in matters of civil rights. The case is still pending. The constitutional validity of PIPEDA was also challenged before the Federal Court in *State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada and Attorney General of Canada*, 2010 F.C. 736. In that case, the Federal Court held that it did not need to address the constitutional questions, considering that the case could be disposed of on other grounds. For a complete analysis on the constitutionality question, see Michel Bastarache, *The Constitutionality of PIPEDA: A Re-consideration in the Wake of the Supreme Court of Canada’s Reference re Securities Act*, June 2012.

20. In its Report on Bill C-6, the Standing Senate Committee on Social Affairs, Science and Technology heard from health sector representatives who described how the CSA Model Code was developed over years of intense negotiation among a widely representative set of stakeholders, including industry associations, government members, privacy commissioners and consumer protection associations. However, witness testimony indicated that groups representing the health sector did not participate in this process in a meaningful way. Thus, it was implied that the Code might not contain adequate provisions for the protection of personal health information.

21. *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.

23. Although Canada’s anti-spam law has been passed, it is not yet in force. The date for the Act’s coming into force are to be set by an order of the Governor in Council. For more information, see Government of Canada, *Canada’s Anti-Spam Legislation*.

24. PIPEDA essentially comprises two parts. Part 1, Protection of Personal Information in the Private Sector, creates rules for the collection, use and disclosure of, as well as access to, personal information in the private sector. Part 2, Electronic Documents, provides for the use of electronic alternatives where federal laws now provide for the use of paper to record or communicate information.


26. PIPEDA, ss. 7(3)(c.1), 7(3)(d)(ii) and 7(3)(i).


29. Bill C-12, c. 5.

30. Ibid., c. 7.

31. Ibid., c. 8.

32. Ibid., cc. 11–14, 16 and 18.

33. ETHI did undertake a study on the efforts and the measures taken by social media companies to protect the personal information of Canadians; however, its recommendations did not include calls for legislative change. ETHI, *Privacy and Social Media in the Age of Big Data*, Fifth Report, 1st Session, 41st Parliament, April 2013.

APPENDIX A – THE 10 PRIVACY PRINCIPLES FROM THE CANADIAN STANDARDS ASSOCIATION MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION

1. Accountability
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the following principles.

2. Identifying Purposes
The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. Consent
The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. Limiting Collection
The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure, and Retention
Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be retained only as long as necessary for fulfilment of those purposes.

6. Accuracy
Personal information shall be as accurate, complete, and up-to-date as necessary for the purpose for which it is to be used.

7. Safeguards
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness
An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. Individual Access
Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging compliance
An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization’s compliance.

NOTES

* Source: Office of the Privacy Commissioner of Canada, “Privacy Principles,” Legal information related to PIPEDA.