LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

BACKGROUND PAPER

CANADA'S FEDERAL PRIVACY LAWS

Publication No. 2007-44-E

17 November 2020

Revised by Alexandra Savoie and Maxime-Olivier Thibodeau

Parliamentary Information and Research Service

AUTHORSHIP

16 November 2020	Alexandra Savoie	Economics, Resources and International Affairs Division
	Maxime-Olivier Thibodeau	Economics, Resources and International Affairs Division
1 October 2013	Miguel Bernal-Castillero	Economics, Resources and International Affairs Division
25 September 2008	Nancy Holmes	Law and Government Division

ABOUT THIS PUBLICATION

Library of Parliament Background Papers provide in-depth studies of policy issues. They feature historical background, current information and references, often anticipating 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.

This publication was prepared as part of the Library of Parliament's research publications program, which includes a set of publications, introduced in March 2020, addressing the COVID-19 pandemic. Please note that, because of the pandemic, all Library of Parliament publications will be released as time and resources permit.

Canada's Federal Privacy Laws
(Background Paper)

Publication No. 2007-44-E

Ce document est également publié en français.

CONTENTS

EXECUTIVE SUMMARY

The right to privacy is recognized as a quasi-constitutional right in Canada. At the federal level, two pieces of legislation provide some privacy protections: the *Privacy Act*, which applies to the public sector, and the *Personal Information Protection and Electronic Documents Act*, which applies to the private sector.

This background paper gives an overview of these two laws, examining their history and various efforts to modernize them over the years as Canadian society has become increasingly reliant on digital technologies.

CANADA'S FEDERAL PRIVACY LAWS

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*[1] and the *Personal Information Protection and Electronic Documents Act* (PIPEDA)[2] – 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 260 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 in all provinces except those that have "substantially similar" private-sector privacy laws and to organizations under federal jurisdiction (e.g., banks and telecommunications firms) anywhere in Canada. PIPEDA also protects employee information, but only in federally regulated sectors.

This paper provides an overview of the federal landscape with respect to privacy laws, their legislative history and the need for modernization to make them better suited to the digital era.

2 HISTORY OF PRIVACY LEGISLATION

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,[3] 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*,[4] 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*.[5] The Convention required Council of Europe 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* (OECD Guidelines) in order to harmonize the data protection practices of member countries by means of minimum standards for handling personal information.[6] 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.[7]

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 applied only to the actions of governments and government agencies.[8] 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 CSA Model Code for the Protection of Personal Information (Model Code) (see the appendix) 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 1995 required all member countries to adopt or adapt national data protection laws to comply with the Union's Directive on Data Protection.[9] 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 2016, the European Union adopted the General Data Protection Regulation (GDPR), which replaced the 1995 directive. Member countries were given two years to fully implement the GDPR domestically.[10] The GDPR officially came into force in May 2018. Chapter V of the GDPR concerns transfers of personal data to third countries or international organizations. Article 45 of this chapter provides that a transfer may occur without specific authorization if it is established that the country or international organization in question ensures an adequate level of protection.

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 the department noted that ensuring consumer confidence was essential to the growth of the information economy.[11] 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."[12] 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,[13] to resolve problems and oversee compliance with the legislation.

The *Privacy Act* applies to the federal government departments and agencies set out in the Schedule to the Act and to Crown corporations and their wholly owned subsidiaries, as defined in section 83 of the *Financial Administration Act*.[14]

Section 3 of the Act defines "personal information" as 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). Section 4 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. In addition, section 5 provides that, 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. In the interests of transparency

and openness, government institutions are required by sections 10 and 11 to publish indexes indicating all of the personal information banks maintained by these institutions.

Section 8 states that 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. 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).

Under sections 12 to 17 of the Act, everyone in Canada has the right to apply for access to personal information about himself or herself that is held by the federal government. Moreover, pursuant to section 12(2)(a), if an individual is not satisfied with the accuracy of the information obtained, he or she may seek to have the inaccuracies corrected. If such a request is refused, the applicant is entitled under section 12(2)(b) to require that a notation be attached to the information describing any corrections requested but not made. The Act also provides, in sections 18 to 28, 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.

Pursuant to sections 29 and 30, if an applicant is not satisfied with the action of a government institution, a complaint can be made to the Privacy Commissioner. On the basis of a complaint, the Commissioner conducts an investigation and issues his or her findings.

Under section 35(1) of the Act, if the Commissioner finds the complaint is well-founded, he or she provides the head of the government institution that has control of the personal information with a report containing the findings and any recommendations he or she considers appropriate. The Commissioner may also ask the institutional head to, within a specified time, give him or her notice of any action taken or proposed to implement the recommendations or reasons why no such action was taken.

Under section 37(1), the Commissioner may also, at his or her discretion, carry out investigations of certain federal institutions to ensure compliance with sections 4 to 8 of the Act (the rules for the collection, retention, disposal and protection of personal information). Findings that the Commissioner considers are in the public interest are, further to section 37(4), published in the Privacy Commissioner's Annual Report to Parliament.[15]

Individuals who are denied access to their personal information by a federal institution may, after completing the complaint process with the Commissioner, file an application for judicial relief to the Federal Court, as provided for in sections 41 to 52.

In addition to investigating complaints about the operation of the *Privacy Act*, the Privacy Commissioner can, under section 60 carry out special studies referred to the Commissioner by the Minister of Justice.[16]

3.1.1 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 committee), the Privacy Commissioner of Canada at the time, Jennifer Stoddart, presented the committee with a comprehensive set of proposals for changes to the *Privacy Act*.[17] 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 enhance the government's responsibility and accountability for the personal information in its control. Ms. Stoddart later published an addendum to the document, in which she provided additional comments in the areas of national security, transborder data flows, data breach notification and legislative coverage of the Act.[18]

In response to these documents and the need for reform, the committee commenced a review of the *Privacy Act* in the spring of 2008.

In 2016, the committee undertook a new study of the Act. During this study, Ms. Stoddart's successor as Privacy Commissioner, Daniel Therrien, presented to the committee his many recommendations for reforming the Act, some of which echoed those of his predecessor.

3.1.1.1 Statutory Review of 2008–2009

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.[19] In addition to recognizing that "a complete overhaul of the Act is in fact warranted," the committee made the following specific recommendations:

- give the Office of the Privacy Commissioner a clear public education mandate;
- strengthen the annual reporting requirements of government departments and agencies so that they report to Parliament on a broader spectrum of privacy-related practices;
- introduce provisions requiring proper security safeguards for the protection of personal information; and
- introduce provisions for an ongoing five-year parliamentary review of the Act.

In its report, the committee also supported the Commissioner's recommendation to eliminate the restriction by which the *Privacy Act* applied 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 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, individuals have no recourse to the courts when they believe government institutions have inappropriately collected, used or disclosed personal information. 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 suggested should change.

Other major changes to the *Privacy Act* proposed in 2008–2009 concerned 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 have for several years now asked 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. No such provision has yet been added to the Act.

In its response to the report and recommendations presented by the committee in June 2009, 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."[20]

No legislation was put forth to substantively amend the *Privacy Act* following the statutory review of 2008–2009.

3.1.1.2 Statutory Review of 2016

In March 2016, the committee began a new study of the *Privacy Act*. In a report published in December 2016, the committee supported most of the legislative amendments that the Privacy Commissioner had recommended and shared with

the committee as part of this statutory review.[21] A number of Mr. Therrien's recommendations were similar to those made by his predecessor during the statutory review of 2008–2009. In its report, the committee recommended, among others, the following measures:

- expand the purpose clause to strengthen the quasi-constitutional nature of the right to privacy;
- amend the definition of "personal information" in the Act to ensure it is technological-neutral and include unrecorded information;
- amend the Act to explicitly require institutions to safeguard personal information and set out the consequences for failure to safeguard them;
- establish an explicit requirement for government institutions to report material breaches of personal information similar to that in PIPEDA;
- amend the Act, which allows a federal institution to collect personal information that "relates directly to an operating program or activity of the institution," to require federal institutions that collect and retain personal information to meet the criteria of necessity and proportionality; and
- grant the Privacy Commissioner the discretionary power to discontinue or decline complaints on specified grounds, including if they are frivolous, vexatious or made in bad faith.

The committee also considered the issue of an appropriate oversight model. Despite the various viewpoints expressed, a consensus emerged from the testimony: the current ombudsman model, with its recommendation powers, is not effective.

Under the ombudsman model, once an investigation is complete, the Commissioner can make only non-binding recommendations to a federal institution. Mr. Therrien recommended switching to an order-making model that would give the Privacy Commissioner the power to issue orders to federal institutions that are not fulfilling their duties under the Act. Such a model would allow federal institutions that wish to challenge an order from the Commissioner to file an application for judicial review with the Federal Court.

Other witnesses advocated for a hybrid oversight model. This model would enable the Office of the Commissioner to make binding recommendations to the government, without, however, being able to order specific measures. A hybrid model would also allow federal institutions that decide not to implement the recommendations to apply to the Federal Court for a declaration that they are not required to do so. The hybrid model would maintain the more informal and flexible character of the current ombudsman model.

In its 2016 report, the committee recommended the order-making model.
It also recommended other changes to the Act, including new measures to increase transparency regarding personal information-sharing agreements (e.g., between the

federal government and a provincial government or foreign government). In addition, it recommended requiring this information sharing to be governed by written agreements that can be reviewed by the Commissioner and including in the Act a requirement to consult with the Office of the Commissioner about draft legislation and regulations with privacy implications.

Finally, the committee encouraged the federal government to consider expanding judicial recourse and remedies under the Act, extending the scope of the Act to all federal government institutions, including ministers' offices and the Prime Minister's Office, extending the right of access to personal information to foreign nationals and limiting exemptions to access to personal information requests under the Act.

In April 2017, in its response to the committee's report and recommendations, the government stated that it "is mindful of the Commissioner's warnings about the risks of antiquated law in this area" and that it was conducting "a thorough review towards modernizing the *Privacy Act*" in order to "examine options for reforming this quasi-constitutional statute that touches almost every function of government."[22]

No bill to substantively amend the Act was introduced following the 2016 statutory review. However, in 2019, the government announced that it would begin work to modernize the Act. It conducted a preliminary technical engagement on the modernization of the *Privacy Act* during the summer and fall of 2019 and on 16 November 2020, launched an online public consultation.[23]

At the time of writing, no bill to amend the Act had been introduced in the House of Commons.

3.2 THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT*

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.[24] 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,[25] PIPEDA's implementation occurred in three stages, starting on 1 January 2001:

- 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.
- On 1 January 2004, the provisions of the Act were extended more broadly to include all private-sector organizations in Canada that collect, use or disclose personal information as part of their commercial activities, even if they operate only within a single province.

However, if a province has enacted legislation that has 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 Alberta, British Columbia and Quebec have adopted legislation that has been deemed "substantially similar" to PIPEDA. In these three provinces, PIPEDA applies only to federally regulated private-sector organizations and to personal information obtained in the course of interprovincial or international transactions. Other organizations are subject to the provincial legislation.

New Brunswick, Nova Scotia, Ontario and Newfoundland and Labrador have laws that are substantially similar to PIPEDA with respect to the custodianship of personal health information. Therefore, PIPEDA does not apply to personal health information in these provinces, but does apply to other private-sector organizations and to any federally regulated organization and any organization engaging in transactions beyond the borders of a single province.

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 (Model Code) (section 5 and Schedule 1 of the Act – see the appendix). 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 (section 5(1) and the seventh principle of the Model Code).

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.[26] 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.[27] The anti-spam legislation complements 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 shares enforcement responsibilities with the Canadian Radio-television and Telecommunications Commission and with the Competition Bureau.

In June 2015, Parliament passed Bill S-4, the Digital Privacy Act, which amended PIPEDA.[28] This bill clarified PIPEDA's wording on consent. The bill added a provision stating that consent 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" (section 6.1 of PIPEDA). It also gave new powers to

the Commissioner, including the ability to enter into compliance agreements with organizations subject to PIPEDA to ensure they meet their obligations under the Act.

Bill S-4 also added a new section to PIPEDA, creating a mandatory personal information security breach reporting regime (section 10.1 of PIPEDA). Under this regime, organizations subject to PIPEDA must take certain steps in case of a security breach involving personal information under their control (e.g., inform the Commissioner). Failure to meet the requirements of section 10.1 of PIPEDA is an offence under the Act and liable to a fine not exceeding $100,000 (section 28). The regime has been in effect since 1 November 2018.

In addition, Bill S-4 allowed the collection, use and disclosure of personal information without an individual's consent in a number of new situations (e.g., for fraud detection and prevention activities or investigations, or business transactions). It also extended the period within which a complainant may apply to the Federal Court for a hearing on matters related to the complaint or cited in a report of the Commissioner from 45 days to one year (section 14 of PIPEDA).

3.2.1 Proposed Amendments to 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 to review Part 1 of the Act, Protection of Personal Information in the Private Sector every five years.[29] However, PIPEDA has undergone only two statutory reviews since it came into force in 2001.

3.2.1.1 Statutory Review of 2006–2007

The first scheduled review of PIPEDA was conducted by the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the committee) between November 2006 and February 2007. A report including 25 recommendations was presented in May 2007.[30]

In its report, the committee did not recommend major changes to the legislation. However, the committee noted 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 Alberta and British Columbia 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).[31] The new collection power in section 7(1)(e) troubled privacy advocates, including the federal Privacy Commissioner at the time, Jennifer Stoddart, who felt that the provision had the undesirable effect of requiring the private sector to carry out law enforcement activities without the accountability that public institutions provide.[32] This PIPEDA provision remains in force.

The most comprehensive recommendation in the 2007 report was made in relation to the duty of private sector organizations to notify individuals in instances of security breaches of their personal information holdings. 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, in its 2007 report, 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 changes were needed at the 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.[33]

On 25 May 2010, the government introduced Bill C-29, An Act to amend the Personal Information Protection and Electronic Documents Act, but this bill died on the *Order Paper* when the 40th Parliament was dissolved. On 29 September 2011, the government introduced a very similar bill, Bill C-12.[34]

Bill C-12 included several of the amendments to PIPEDA suggested by the committee, including changes aimed at clarifying consent, making consent 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.[35]

Bill C-12 also sought to change the consent requirements pertaining to the personal information of employees of federal works, undertakings or businesses, allowing them to collect, use and disclose employee personal information without consent if this information is needed to "establish, manage or terminate" employment, as long as the employee concerned has been notified in advance that the information is being collected, used, or disclosed and why.[36]

Bill C-12 also created other exceptions to consent requirements, including when the personal information is requested to perform policing services. It also expanded 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.[37]

Most significantly, Bill C-12 introduced new breach notification provisions, placing new responsibilities on organizations to report instances where the personal information they hold is subject to a security breach.[38] As noted above, when Bill S-4 was passed in 2015, it established a mandatory reporting regime for security breaches involving personal information. One of the security breach reporting obligations is the duty to notify any individual affected "if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual" (section 10.1(3) of PIPEDA)

Bill C-12 did not advance beyond first reading after being introduced in September 2011. It died on the *Order Paper* at the end of the 1st Session of the 41st Parliament on 13 September 2013. Multiple aspects of Bill C-12 were reprised in Bill S-4, which added to PIPEDA a regime for reporting personal information security breaches.[39]

In May 2013, the then Privacy Commissioner, Jennifer Stoddart, published a comprehensive paper in which she argued for an in-depth reform of PIPEDA, one that went beyond what was proposed in Bill C-12.[40] In her document, Ms. Stoddart argued for stronger enforcement 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.

3.2.1.2 Statutory Review of 2017–2018

The committee conducted the second statutory review of PIPEDA from February 2017 to February 2018. The resulting report included 19 recommendations.[41]

The committee examined the future of meaningful consent as a fundamental principle of PIPEDA. It relied on the evidence it heard and a study of consent conducted by the Office of the Privacy Commissioner in 2016.[42] Central to the debate was the relevance of explicit consent in the digital era, when the increasing complexity of online interactions and the growing number of uses of personal information can make meaningful consent more difficult to obtain.

Some witnesses argued that meaningful consent in online transactions is somewhat illusory because conditions of use are generally buried in long and vague legal texts presented on a "take it or leave it" basis. For their part, business representatives said the consent model poses problems because it could hinder innovation and deprive consumers of the potential benefits of data use (e.g., customization of products and services).

Still, most witnesses were of the view that consent, in one form or another, must remain a key part of PIPEDA. Some supported an approach focused on the components of explicit consent and suggested a risk-based model of consent, in which consent is necessary only when there is a risk of harm to the individual. Others feared that such a model could lead to over-collection of personal information. Many witnesses proposed keeping consent as the basis for PIPEDA, noting that the principle of consent currently entrenched in the legislation is rigorous and flexible enough to handle new uses of personal information in the digital era.

The committee recommended that consent remain at the heart of the personal information protection regime, but that it should be strengthened and clarified through additional measures where possible or necessary. It also recommended that PIPEDA be amended to explicitly provide for opt-in consent as the default for any use of personal information for secondary purposes.

With regard to the Commissioner's powers under PIPEDA, the committee referenced the recommendation it made in its 2016 report on the *Privacy Act*: adopt an order-making oversight model that enables the Commissioner to issue orders.

Most of the witnesses, including the Privacy Commissioner, advocated changing the ombudsman model to grant the Commissioner certain powers, including the power to make orders and impose monetary penalties or fines for substantial or systemic non-compliance with the obligations contained in PIPEDA. A number of organizations governed by PIPEDA were in favour of maintaining the current ombudsman model and against granting the Commissioner order-making powers. However, if such powers were to be conferred, they would support strict limits on their scope.

In light of the evidence it heard, the committee recommended that PIPEDA be amended to give the Privacy Commissioner enforcement powers, including the power to make orders and impose fines for non-compliance with obligations under the Act.

The committee made a number of other recommendations to the government, including the following:

- take measures to improve algorithmic transparency;
- study the issue of revocation of consent;
- amend PIPEDA to clarify the terms under which personal information can be used to serve legitimate business interests;
- examine the best ways of protecting depersonalized data;
- consider implementing specific rules of consent for minors and regulations governing the collection, use and disclosure of minors' personal data;
- amend PIPEDA to provide a right to data portability;
- consider including in PIPEDA a framework for a right to erasure and a right to de-indexing of data;
- consider amending PIPEDA to strengthen and clarify organizations' obligations respecting the erasure of personal information;
- amend PIPEDA to make privacy by design a central principle of the Act; and
- amend PIPEDA to allow the Privacy Commissioner to choose which complaints to investigate.

Finally, the committee considered the issue of PIPEDA's adequacy under the European Union's GDPR. For now, Canada is still considered to have an adequate data protection regime, but a new assessment may produce a different result, given that federal privacy legislation has not been modernized despite many calls for reform. Moreover, the Commissioner's lack of enforcement powers appears to be one of PIPEDA's greatest weaknesses if it is to be seen as adequate by European Union standards.

In its response to the committee's report, the government stated that it agreed with the committee that "changes are required to our privacy regime," but it noted that, to fuel innovation while fostering public trust, the government must continue its conversation with stakeholders. Regarding the Commissioner's powers, the government indicated that it had to study the range of compliance and enforcement models available and the repercussions they could have on the Commissioner's mandate, the principles of fundamental justice and the risks associated with increased enforcement powers (e.g., the potential impact on open dialogue between the Office of the Commissioner and the organizations subject to PIPEDA).[43]

The committee reiterated its recommendations for modernizing PIPEDA in its preliminary and final reports of its study on the breach of personal information involving Cambridge Analytica and Facebook, published in December 2018 and June 2019, respectively. It also recommended further amendments to address gaps in PIPEDA.[44]

On 17 November 2020, the Minister of Innovation, Science and Industry introduced in the House of Commons Bill C-11, An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential amendments to other Acts. This bill would reform PIPEDA and implement Canada's Digital Charter.[45]

4 CALLS FOR REFORM: THE PRIVACY COMMISSIONER'S RECENT COMMENTS

The current Privacy Commissioner, Daniel Therrien, has long called for changes to federal privacy laws.

In November 2019, the Commissioner and his provincial and territorial counterparts issued a joint resolution urging governments to modernize access to information and privacy laws. In their resolution, the Commissioner and his counterparts noted the following:

> Most Canadian access and privacy laws have not been fundamentally changed since their passage, some more than 35 years ago. They have sadly fallen behind the laws of many other countries in the level of privacy protection provided to citizens.[46]

In December 2019, the Office of the Privacy Commissioner of Canada released its annual report for 2018–2019, entitled *Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy*. In this report, Mr. Therrien pointed out that, like his predecessors, he has been calling for an overhaul of Canada's federal private- and public-sector privacy laws for several years. He added that privacy is a precondition for exercising other fundamental rights, including freedom, equality and democracy. Mr. Therrien argued that new privacy legislation should be rights-based and should define privacy protection in its broadest sense – for instance, by describing it as freedom from unjustified surveillance.[47]

According to the Commissioner:

- the legislation should be able to endure over time, meaning that it will remain relevant despite technological changes;
- the legislation that applies to the private sector should truly and firmly put an end to self-regulation;

- the legislation that applies to the public sector should apply the principles of necessity and proportionality to the collection and retention of personal information in order to prevent over-collection; and
- the legislation should contain enforcement mechanisms that ensure individuals have a quick and effective remedy to protect their privacy rights, including order-making and fine-issuing powers for the Office of the Commissioner and any other enforcement body.[48]

At present, federal privacy laws emphasize data protection rather than the exercise of privacy rights. Consequently, the Commissioner suggested amending federal privacy laws to recognize privacy as a human right, as does, for example, the EU's GDPR. Mr. Therrien argued, "Modernized privacy legislation should start by defining privacy in its proper breadth and more formally codify its quasi-constitutional status."[49]

Lastly, the Commissioner underscored that one of the required improvements to federal privacy laws is to empower the Privacy Commissioner of Canada to conduct proactive inspections (rather than follow up on reports of breaches), make binding orders and impose penalties for non-compliance with the legislation. Mr. Therrien noted that such powers already exist in some provinces, including British Columbia and Alberta (orders), and in other countries, such as the United States and the European Union countries (orders and penalties).

In his 2018–2019 annual report, the Commissioner further proposed granting Canadians an independent right of action in the courts to seek remedies for violations of their privacy rights.[50]

More recently, in May 2020, the Commissioner and his provincial and territorial counterparts released a joint statement to set out some principles that should be adhered to in developing any contact tracing technology in response to the coronavirus disease 2019 (COVID-19) pandemic. These principles include the necessity and proportionality, as well as transparency. In their statement, the commissioners state, "While applicable privacy laws must be observed, some of them do not provide an effective level of protection suited to the digital environment."[51] During an appearance before a House of Commons standing committee in May 2020, the Commissioner explained that many of the principles set out in the joint statement of May 2020 are not part of the current federal legislation and that he believes these principles should have force of law.[52]

Finally, in his annual report for 2019–2020, published in October 2020, the Commissioner reiterated the need to modernize Canada's privacy laws to better protect Canadians in the digital era. He remarked that the COVID-19 pandemic has made the shortcomings of the current legislative framework more obvious than ever.[53]

5 CONCLUSION

Aside from a few technical amendments, including the changes to PIPEDA following passage of Bill S-4, Canada's federal privacy laws have not been overhauled since they were first enacted. Despite many calls for reform over the years, these laws remain, for the moment, largely in their original form.

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 remains a 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 which individuals or organizations.

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

1. *Privacy Act*, R.S.C. 1985, c. P-21.
2. *Personal Information Protection and Electronic Documents Act* [PIPEDA], S.C. 2000, c. 5.
3. Task Force on Privacy and Computers, *Privacy and Computers: A Report of a Task Force*, Ottawa, 1972.
4. *Access to Information Act*, R.S.C. 1985, c. A-1.
5. Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS No. 108, Strasbourg, 28 January 1981.
6. Organisation for Economic Co-operation and Development [OECD], *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines), 23 September 1980.
7. OECD, *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, revised 11 July 2013. The new 2013 OECD 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 Guidelines.

8. Quebec was the first province to pass privacy legislation that applied to the private sector. The *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).

9. EUR-Lex, *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*, Official Journal L 281, 23 November 1995.

10. Official Journal of the European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council*.

11. Taskforce on Electronic Commerce, *A Cryptology Policy Framework for Electronic Commerce – Building Canada's Information Economy and Society*, Industry Canada, Ottawa, February 1998.

12. John Grace, "The ethics of information management," in *Do Unto Others: Proceedings of a Conference on Ethics in Government and Business*, ed. Kenneth Kernaghan, Institute of Public Administration of Canada, Toronto, 1991, p. 95.

13. 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.

14. *Financial Administration Act*, R.S.C. 1985, c. F-11.

15. Summaries of findings under the *Privacy Act* are available at the OPC website. See OPC, "Investigations into federal institutions", *OPC actions and decisions*

16. Completed audit reports are available at OPC, "Audits," *OPC actions and decisions*.

17. OPC, *Government Accountability for Personal Information: Reforming the* Privacy Act, June 2006.

18. OPC, *Addendum to Government Accountability for Personal Information: Reforming the* Privacy Act, April 2008.

19. House of Commons, Standing Committee on Access to Information, Privacy and Ethics [ETHI], *The* Privacy Act*: First Steps Towards Renewal*, Tenth Report, 2nd Session, 40th Parliament, June 2009.

20. Rob Nicholson, Minister of Justice and Attorney General, Government Response to the Tenth Report of the Standing Committee on Access to Information Privacy and Ethics: *The* Privacy Act*: First Steps Towards Renewal*, 9 October 2009.

21. ETHI, *Protecting the Privacy of Canadians: Review of the* Privacy Act, Fourth Report, 1st Session, 42nd Parliament, December 2016; ETHI, *Evidence*, 10 March 2016 (Daniel Therrien, Privacy Commissioner of Canada); and OPC, Privacy Act *Reform in an Era of Change and Transparency*, 22 March 2016.

22. Jody Wilson-Raybould, Minister of Justice, *Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics*, 12 April 2017.

23. Department of Justice, *Modernizing Canada's* Privacy Act*: What We Heard Report*; and Department of Justice, "Government of Canada launches public consultation on the *Privacy Act*," News release, 16 November 2020.

24. 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, to be heard by the Court of Appeal of Quebec, the federal government has exceeded its jurisdiction under PIPEDA in that it interferes with Quebec's constitutional competence in matters of civil rights. However, the Court of Appeal of Quebec never ruled on this case. The constitutional validity of PIPEDA was also challenged before the Federal Court in *State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada*, 2010 FC 736. In that case, the Federal Court held that it did not need to address the constitutional questions, as the case could be disposed of on other grounds.

25. 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 Canadian Standards Association Model Code (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 Model Code might not reflect the realities of the sector or contain adequate provisions for the protection of personal health information. See Senate, Standing Committee on Social Affairs, Science and Technology, *Fourteenth Report*, 1st Session, 37th Parliament, 14 December 2001.

26. *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.

27. See Terrence J. Thomas and Erin Virgint, *Legislative Summary of Bill C-28: 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*, Publication no. 40-3-C28-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 15 November 2012.

28. 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 (S.C. 2015, c. 32). For more information, see Dara Lithwick, *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*, Publication no. 41-2-S4-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 11 June 2014.

29. 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 or transactions.

30. ETHI, *Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)*, Fourth Report, 1st Session, 39th Parliament, May 2007.

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

32. OPC, *Statutory Review of the PIPEDA: Background Information on the OPC's Consultation*, 27 November 2006, cited in ETHI (2007), pp. 26–27.

33. 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)*, 17 October 2007.

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

35. Bill C-12, cl. 5.

36. Ibid., cl. 7.

37. Ibid., cl. 8.

38. Ibid., cls. 11–14, 16 and 18.

39. Lithwick (2014).

40. OPC, *The Case for Reforming the* Personal Information Protection and Electronic Documents Act, May 2013.

41. ETHI, *Towards Privacy by Design: Review of the* Personal Information Protection and Electronic Documents Act, Twelfth Report, 1st Session, 42nd Parliament, February 2018.

42. Ibid., p. 5; and OPC, *Consent and privacy: A discussion paper exploring potential enhancements to consent under the* Personal Information Protection and Electronic Documents Act, May 2016.

43. Navdeep Bains, Minister of Innovation, Science and Economic Development, Government Response to the Twelfth Report of the Standing Committee on Access to Information, Privacy and Ethics.

44. ETHI, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process*, Sixteenth Report, 1st Session, 42nd Parliament, June 2018; and ETHI, *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly*, Seventeenth Report, 1st Session, 42nd Parliament, December 2018.

45. Bill C-11, An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts, 2nd Session, 43rd Parliament; and Innovation, Science and Economic Development Canada, *Canada's Digital Charter: Trust in a digital world*.

46. OPC, "Canada's access to information and privacy guardians urge governments to modernize legislation to better protect Canadians," News release, 6 November 2019.

47. OPC, *Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy*, 2018–2019 Annual Report, pp. 2–3.

48. Ibid., pp. 3–5.

49. Ibid., p. 11.

50. Ibid., p. 13.

51. OPC, "Supporting public health, building public trust: Privacy principles for contact tracing and similar apps," Joint Statement by Federal, Provincial and Territorial Privacy Commissioners, 7 May 2020.

52. House of Commons, Standing Committee on Industry, Science and Technology, *Evidence*, 1505, 29 May 2020 (Daniel Therrien, Privacy Commissioner of Canada).

53. OPC, *Privacy in a Pandemic: 2019–2020 Annual Report to Parliament on the* Privacy Act *and* Personal Information Protection and Electronic Documents Act, 8 October 2020.

APPENDIX – *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT* FAIR INFORMATION PRINCIPLES*

ACCOUNTABILITY

- An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.

IDENTIFYING PURPOSES

- The purposes for which personal information is being collected must be identified by the organization before or at the time of collection.

CONSENT

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

LIMITING COLLECTION

- The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.

LIMITING USE, DISCLOSURE, AND RETENTION

- Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.

ACCURACY

- Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.

SAFEGUARDS

- Personal information must be protected by appropriate security relative to the sensitivity of the information.

OPENNESS

- An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.

INDIVIDUAL ACCESS

- Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and 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.

CHALLENGING COMPLIANCE

- An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be addressed to the person accountable for the organization's compliance with PIPEDA, usually their Chief Privacy Officer.

NOTES

* Source: Office of the Privacy Commissioner of Canada, *PIPEDA fair information principles*.