PRB 07-44E

CANADA'S FEDERAL PRIVACY LAWS

Nancy Holmes
Law and Government Division

28 November 2007

PARLIAMENTARY INFORMATION AND RESEARCH SERVICE
SERVICE D'INFORMATION ET DE RECHERCHE PARLEMENTAIRES

TABLE OF CONTENTS

Page

CANADA
LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

CANADA'S FEDERAL PRIVACY LAWS

INTRODUCTION

Classically understood as the "right to be left alone," privacy in today's high-tech world has taken on a multitude of dimensions. To experts in this area, privacy is equated 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 about control – what is known about them and by whom.

Privacy protection in this country essentially focuses on safeguarding personal information. Drawing upon generally accepted fair information practices, federal data protection laws 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 is an unacceptable privacy intrusion to one person, may not be to another.

This paper will canvass the federal landscape in terms of privacy legislation, its legislative history, and the need for modernization at a time when technology and terrorism are rapidly transforming the world in which we live.

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,[1] Canada enacted the first federal public sector privacy protection in Part IV of

(1) Department of Communications and Department of Justice, *Privacy and Computers: A Report of a Task Force*, Information Canada, Ottawa, 1972.

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, and in 1983, the current *Privacy Act* came into force along with the *Access to Information Act*. 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 from computers that no longer stood alone, but could communicate with another and exchange information. As a result, various federal and state data protection laws arose in Europe in the 1970s, and in 1980, the Council of Europe enacted the Convention for the Protection of Individuals with regard to the 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. That same year, the Organisation for Economic Co-operation and Development (OECD) released *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (Appendix A) 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 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,[(2)] applied only to the actions of governments and government agencies. While the federal government, and indeed the federal Privacy Commissioner, were content at

(2) Quebec's *Act Respecting the Protection of Personal Information in the Private Sector*, 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 (not just with respect to their commercial activities).

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 (Appendix B) 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 towards 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. In terms of non-member countries, such as Canada, Article 25 of the Directive prohibits member countries (and businesses within those countries) from transferring personal information to a non-member of the European Union if that country's laws do not adequately guarantee protection of that information.(3)

In January 1998, Industry Canada and the Department of Justice 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 paper 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

(3) 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.

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 as Bill C-6 in October 1999 and came into force on 1 January 2001.

FEDERAL PRIVACY LAWS

A. The *Privacy Act*

The *Privacy Act* came into force, along with the *Access to Information Act*, on 1 July 1983. The Act is a data protection law, once described as an "information handler's code of ethics." The law has three basic components: 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 in terms of how it collects, maintains, uses and discloses personal information under its control; and it puts in place an independent ombudsman, the Privacy Commissioner,(4) to resolve problems and oversee compliance with the legislation. The *Privacy Act* applies only to those federal government departments and agencies set out in the Schedule to the Act.

Personal information under the Act includes any information about an identifiable individual, recorded in any form (i.e., video or audiotape, or any electronic information medium), including information about one's age, education, medical or criminal 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. 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. 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.

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

(4) The Privacy Commissioner is an Officer of Parliament who is appointed by Governor in Council for a maximum of seven years.

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).

Everyone in Canada has the right to apply for access to personal information about him or her that is held by the federal government. 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 may require that a notation be attached to the information describing any corrections requested but not made. 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. If an applicant is not satisfied with the action of a government institution, a complaint can be made to the Privacy Commissioner. When this recourse is unsuccessful, an application for judicial relief can be made to the Federal Court.

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.

B. 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.[(5)] Essentially, PIPEDA 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.

---

(5) 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 based on its general power to regulate trade and commerce. However, according to a constitutional challenge by the Quebec government currently before the courts, the federal government has exceeded its jurisdiction under PIPEDA in that it interferes with Quebec's constitutional competence in matters of civil rights.

PIPEDA came into effect in three stages:

- 1 January 2001, the Act applied only to the federally regulated private sector (i.e., telecommunications, broadcasting, banking and interprovincial transportation and airline industries). It also covered interprovincial or international trade in personal information.

- 1 January 2002, personal health information became subject to the Act.

- 1 January 2004, the provisions of the Act 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. Where, however, a province enacts 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 Quebec, Alberta, Ontario (with respect to personal health information) and British Columbia have provincial legislation that has been accorded the status of "substantially similar" to PIPEDA.

The delay in the application of PIPEDA to personal health information resulted from Senate amendments to Bill C-6, PIPEDA, before it became law. In its December 1999 report, the Standing Senate Committee on Social Affairs, Science and Technology observed a considerable amount of uncertainty within the health sector surrounding the application of the privacy protection provisions of the bill to personal health information. Indeed, witnesses who appeared before the Committee criticized the bill for its lack of clarity and its inappropriateness in respect of health information.(6) The Committee therefore recommended a suspension of the application of the law to personal health information for a period of one year following the coming into force of the bill. It was felt that this would provide time for the government and affected parties to address many of the concerns through consultations and the formulation of appropriate solutions. The outcome of this delayed application was a set of guidelines, known as PIPEDA Awareness Raising Tools (PARTS), designed to clarify, by means of a question and answer format, the obligations of the health care community under PIPEDA.(7)

---

(6) For example, the Committee heard that 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 does not contain provisions suitable for the protection of personal health information.

(7) The PARTS initiative was the result of work between the health care community, officials from the Privacy Commissioner's office, Health Canada, Justice Canada and Industry Canada.

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 (Schedule 1 of the Act – see Appendix B). Essentially, organizations are responsible for the protection of personal information and the fair handling of it at all times, throughout the organization and in dealings with third parties. Subject to limited exceptions, they are required to obtain an individual's consent when collecting, using or disclosing the individual's personal information. Purposes for which an organization can collect, use or disclose personal information are to be limited to those that "a reasonable person would consider are appropriate in the circumstances." Personal information can only be used for the purpose for which it was collected and where an organization is going to use it 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. The Commissioner will usually attempt to resolve the matter through persuasion and negotiation; however, in cases where the ombudsman approach fails to work, recourse may be had to the Federal Court for judicial remedies, including orders to comply and damages.

The Commissioner also has the power to audit the personal information management practices of an organization; make public any information relating to an organization's personal information practices when it is in the public interest to do so; enter into agreements with his or her provincial counterparts to coordinate activities; undertake and publish research and develop model contracts for the protection of personal information that is collected, used or disclosed interprovincially or internationally; and develop and conduct information programs to foster public understanding of the provisions of PIPEDA.

CALLS FOR REFORM

In this age of rapidly advancing informational technologies, globalization and heightened security concerns, privacy advocates are calling for immediate reforms to Canada's federal privacy laws. Clearly, there is some merit in a modernized *Privacy Act*, given that it has

basically remained unaltered since coming into force almost 25 years ago.(8) As well, calls have been made for changes to PIPEDA on the basis that it has been in existence for more than five years and provincial private sector legislation has largely surpassed federal standards in many respects.

A. Statutory Review of PIPEDA

Pursuant to section 29 of PIPEDA, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the Committee) undertook a review in 2006-2007 of Part 1 of the Act, Protection of Personal Information in the Private Sector.(9) The Committee held hearings from November 2006 until February 2007 and tabled a report with 25 recommendations in May 2007.(10)

The report did not advocate major changes to the legislation. The Committee was concerned that, as the full implementation of the Act did not come about until January 2004, not every aspect of the law has yet been implemented. Thus, the Committee, for the most part, limited itself to fine-tuning 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/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 canvassing the Quebec, British Columbia and Alberta approaches to privacy protection in the workplace setting, the Committee felt that there is 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

---

(8) The *Federal Accountability Act*, S.C. 2006, c. 9, made some amendments to the *Privacy Act*, including broadening the scope of the Act to include the Offices of the Information and Privacy Commissioner, all Crown corporations and five foundations.

(9) PIPEDA is essentially comprised of 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.

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

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).[11] The new collection power in section 7(1)(e) troubled privacy advocates, including the federal Privacy Commissioner, who felt that the provision has the undesirable effect of requiring the private sector to carry out law enforcement activities without corresponding state accountability.

The most comprehensive Committee recommendation came in relation to breach notification and 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 as major breaches involving personal information are increasingly coming to light in this country. The Committee was also cognizant of the fact that may US states have passed laws requiring that customers be notified when their personal information has been compromised. While the Committee did not endorse "mandatory breach notification," whereby every person whose personal information is compromised would be notified, 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 stressed the need for the investment of more resources to better educate both 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 organizations being fully aware of their obligations under the law.

On 17 October 2007, the Government issued its response to the Committee's report.[12] Essentially, the Government agreed with the Committee that no significant change is needed at this time with respect to PIPEDA. Indeed, most of the Committee's 25 recommendations were accepted. The response does, however, indicate that further consultation is needed in several critical areas before any legislative and policy proposals can be presented for parliamentary consideration.

---

(11) Sections 7(3)(c.1), 7(3)(d)(ii) and 7(3)(i).

(12) See http://www.ic.gc.ca/epic/site/ic1.nsf/en/00317e.html.

B. Proposals for Amending the *Privacy Act*

Numerous privacy commissioners have, over the years, outlined proposals for amending the *Privacy Act*.(13) Indeed, calls for reform go as far back as 1987, when the House of Commons Standing Committee on Justice and the Solicitor General made more than 100 unanimous recommendations for improving the legislation in its report, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*. The House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities also recommended in 1997 that the *Privacy Act* be broadened and strengthened in relation to all issues of privacy within the federal sector.(14)

More recently, the Privacy Commissioner of Canada, Jennifer Stoddart, in June 2006, presented the House of Commons Standing Committee on Access to Information, Privacy and Ethics with a set of proposals for changes to the Act.(15) The Commissioner emphasized that in terms of accountability and transparency in government, the public sector privacy law must ensure that government is both responsible and fully accountable for the personal information in its control. In her view, it is unfortunate that the government currently holds the private sector to a higher privacy standard under PIPEDA than it imposes on its own information practices. A comprehensive review of the *Privacy Act* is therefore warranted particularly when one considers that, contrary to 25 years ago when the *Privacy Act* came into existence, governments today function in a world of globalization and increased information holdings stemming in part from national security concerns.

Among the Commissioner's many recommendations for change is a broader range of fair information practices to govern the federal government's privacy management regime. According to the Commissioner, the Act's current controls on the federal government's information management practices are either too lenient or in many cases simply non-existent. There is a need, for example, for a "necessity test," similar to that under PIPEDA, to ensure that departments and agencies demonstrate a need for the information they are collecting. There also need to be ground rules for data matching of personal information between and within federal government departments and agencies. The Commissioner would like to be given a review and approval function in relation to any data-matching initiative, similar to that used in other

---

(13) See for example, *Privacy Act* Reform: Issue Identification and Review, A Report by the Privacy Commissioner of Canada on Proposed Amendments to the Federal *Privacy Act*, 16 June 2000.

(14) *Privacy: Where Do We Draw the Line?*, report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, April 1997.

(15) *Government Accountability for Personal Information: Reforming the Privacy Act*, June 2006, http://www.privcom.gc.ca/information/pub/pa_reform_060605_e.asp.

jurisdictions such as Australia and New Zealand. Finally, the Act should contain specific legal rules for the protection of personal information in an online context. Reference to the United States' *E-Government Act* of 2002 is made in this regard.

The Commissioner also contends that the *Privacy Act* must mirror its private sector counterpart in terms of enforcement. Currently, the Act allows only complainants or the Privacy Commissioner the right to go to the Federal Court 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. The Privacy Commissioner is an ombudsman and, as such, has no order-making powers with respect to damages caused by government actions in relation to the inappropriate collection, use or disclosure of personal information.

With respect to the outsourcing of government-held information as well as transborder data flows, it is recommended that privacy standards be incorporated into the *Privacy Act* to address these matters. For example, relative to data protection laws in most European countries, Canada has a relatively low standard for the disclosure of personal information to other countries. By way of contrast, the European Union restricts the disclosure of government – held information to those foreign states that provide adequate levels of privacy protection.

Finally, the definition of "personal information" should be expanded to include both recorded and unrecorded information, such as DNA, about identifiable individuals. The Privacy Commissioner's office should have a clearly mandated public education function and be required to report annually on the personal information management practices of government institutions. As well, all individuals about whom the government holds personal information (and not just those persons present in Canada) should have a right of access to, and the ability to correct, that information.

CONCLUSION

The advent of the Internet and the globalization of personal information have brought the issue of privacy protection to a new level of importance. What was once only science fiction is today's reality, and the extent to which legislative protection can keep pace with rapidly advancing technologies remains to be seen. Indeed, the concept of privacy in and of itself is subject to debate. There are advocates who contend that privacy is more than just controlling personal information or being left alone; it is a core human value that defines who we are and how we interact with others in society. Yet 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, as well as private individuals.

APPENDICES

APPENDIX A

OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

BASIC PRINCIPLES OF NATIONAL APPLICATION

7. Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

8. Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

9. Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

10. Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

11. Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

12. Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

13. Individual Participation Principle

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and
- in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

14. Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

Source: http://www1.oecd.org/publications/e-book/930201E.pdf.

APPENDIX B

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

- 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.

- 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.

- 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 shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

- 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.

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

- Safeguards: personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

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

- 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.

- 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.

Source: Canadian Standards Association, http://www.csa.ca/standards/privacy/code/default.asp?articleID=52908language=English.