IN BRIEF

Parliamentary Information and Research Service
Library of Parliament

Nancy Holmes
22 February 2006

The Right to Privacy and Parliament

INTRODUCTION

Classically understood as the "right to be left alone," privacy in today's high-tech world has taken on a multitude of dimensions. In its broadest sense, privacy is equated with the right to enjoy private space, to conduct private communications, to be free from surveillance and to respect the sanctity of one's body. To most people, privacy is about control – what is known about them and by whom.

Privacy protection in this country, however, is focussed on the safeguarding of personal information or data protection. Drawing upon generally accepted fair information practices,(1) federal laws seek to allow, to the greatest extent possible, individuals to decide for themselves 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 extent to which federal privacy laws apply to Parliament; that is, to parliamentary institutions (the House of Commons, the Senate and the Library of Parliament) as well as to parliamentarians (Members of Parliament and Senators). Given that parliamentary data collection, use and disclosure often involve personal information already in the public domain, this paper will also briefly review how federal privacy laws address the issue of publicly available information.

THE APPLICATION OF FEDERAL PRIVACY LAWS TO PARLIAMENT

Canada has two data protection laws at the federal level: the *Privacy Act*(2) and the *Personal Information Protection and Electronic Documents Act* (PIPEDA).(3) The *Privacy Act* is a public-sector law that obliges federal government departments and agencies to respect privacy rights by limiting the collection, use and disclosure of personal information to a set of fair information rules. The Act also gives individuals the right to access and request correction of personal information held about themselves by federal government organizations. Like its public-sector counterpart, PIPEDA codifies a set of fair information principles that apply to the handling of personal information by private-sector organizations in the course of commercial activities. The law also gives individuals the right to access and request correction of personal information held about them by private-sector organizations. Both privacy Acts are subject to oversight by an independent ombudsman, the Privacy Commissioner of Canada, who resolves problems and oversees compliance with the legislation.

Currently, neither federal privacy law applies to Parliament. As noted above, PIPEDA's privacy protection is limited to the collection, use and disclosure of personal information in the private sector, and only in the context of commercial activities. The *Privacy Act* applies only to "government institutions," which are defined (in section 3) as all of the government departments, bodies and offices listed in the Schedule to the Act.

In 1997, the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities recommended that federal data protection legislation should apply to Parliament.(4) In 2000, following a comprehensive review of the *Privacy Act*, the Privacy Commissioner of Canada recommended that the House of Commons and the Senate be included among the list of institutions subject to the Act.(5) There has, however, been no subsequent legislative action in this regard. As a result, parliamentary employees and the general public do not have rights under the Act to their personal information held by a parliamentary institution or parliamentarian.

Arguably, there is always the possibility of privacy infringement claims in relation to Parliament pursuant to sections 7 and 8 of the *Canadian Charter of Rights and Freedoms*.[6] While Canadians have no express constitutional right to privacy, the courts have interpreted sections 7 and 8 of the Charter as guarding against unreasonable invasions of privacy. Section 7 provides for the right to life, liberty and security of the person and the right not to be deprived of these rights except through some form of due process. Section 8 protects against unreasonable search and seizure. The privacy value in these rights, however, has largely been recognized in the criminal law context. It is for this reason, among others, that calls continue to be made for the entrenchment of an explicit and broad right to privacy in the Canadian Constitution.

All that being said, it has generally been the practice of parliamentary institutions and parliamentarians to respect the principles of federal human rights legislation, particularly when the courts have recognized such legislation as quasi-constitutional.[7] As the Supreme Court of Canada pointed out in *Canada (House of Commons)* v. *Vaid*,[8] legislative bodies created under the Constitution "do not constitute enclaves shielded from the ordinary law of the land," and parliamentary privilege only functions to provide "necessary immunity" for legislators to do their work. Thus, although Parliament in its wisdom has chosen not to include itself within the ambit of the federal *Privacy Act*, best polices and practices would certainly dictate that as a public institution accountable to the public, Parliament should strive to conduct itself in a manner consistent with that required of others in terms of protecting the privacy of personal information.

Guidance in the application of fair information practices to the parliamentary context might therefore be drawn from the privacy principles set out in the federal *Privacy Act*. The Act incorporates the basic tenet underlying most data protection laws, which is that an individual's personal information[9] is his or hers to control. The law stipulates that only personal information related directly to an operating program or activity of government may be collected. It also requires that, wherever possible, the information be collected directly from the individual concerned, that the individual be informed of the purpose of the collection, and that the information be used or disclosed only for the purpose for which it was collected unless the individual consents or the legislation provides otherwise.

Reference to PIPEDA might also be helpful in the formulation of any parliamentary privacy policy, particularly as most privacy advocates, as well as the Privacy Commissioner of Canada, view the *Privacy Act* as an inadequate and outdated first-generation privacy law in comparison to the private-sector privacy law.[10] With rapid technological advances, globalization and information outsourcing, the privacy landscape has become much more complex than it was when the *Privacy Act* was enacted in 1983. PIPEDA, among other things, contains a broader definition of "personal information"[11] as well as provisions explicitly covering data matching.[12] Moreover, it has been submitted that many of the problems with the *Privacy Act* could be remedied by adopting the privacy principles under the Canadian Standards Association *Model Code for the Protection of Personal Information*, which forms the basis of PIPEDA's privacy protection. The following 10 privacy principles from the *Model Code* are widely seen within the privacy community as constituting the basic elements of a solid framework for privacy management:

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

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

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

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

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

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

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

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

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

10. *Challenging compliance*: an individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.[13]

FEDERAL PRIVACY LAWS AND PUBLICLY AVAILABLE INFORMATION

A great deal of personal information that is collected, used and disclosed by parliamentary institutions and parliamentarians may be drawn from publicly available sources (e.g., public registries, professional directories, court records). The nature of publicly available information has certainly been altered by today's technological advances (e.g., ease of access to electronic documents, particularly via the Internet, as opposed to traditional hard copies). Data protection statutes have struggled to address the privacy concerns associated with publicly available information, but most laws simply avoid the issue altogether by allowing information that has been released under statutory authority to be reused without consent.[14] The *Privacy Act* has essentially taken this latter approach. Section 69(2) of the Act provides that the use and disclosure rules found in sections 7 and 8 do not apply to personal information that is publicly available. This means, for example, that where a government institution wishes to obtain information that is in the public domain from another government institution, it may do so without having to obtain the consent of the data subject.[15]

PIPEDA, on the other hand, has attempted to address the fact that individuals may have a continuing privacy interest in some of their publicly available personal information. In other words, consent to make personal information available for one purpose, even if that purpose entails making the information public, does not necessarily mean that the consent is implicit for subsequent purposes. Thus section 7(1)(*d*) of PIPEDA allows organizations to collect, use or disclose information that is publicly available without the knowledge or consent of the individual only in accordance with the regulations to the Act. The regulations provide that publicly available information may be collected, used or disclosed without consent where such action is consistent with the primary purpose for which the information was made public, thereby ensuring the tacit agreement of the individual.[16] An example might be the telephone directory, in which individuals allow their name, address and telephone number to appear so that others may contact them. Thus, it would arguably be reasonable to allow other organizations to collect, use and disclose this information for a similar purpose without adding the requirement to obtain consent for these subsequent collections, uses or disclosures.[17] The consent requirement should apply, however, to any purpose other than that primary one. Put another way, secondary or commercial collection, use and disclosure of publicly available information could be subject to the requirement of consent under PIPEDA.[18]

CONCLUSION

Parliament, its institutions, members and staff will most certainly encounter situations where choices have to be made about the handling of personal information. In making these choices, reference to the fair information principles set out in Canada's privacy statutes may prove helpful. Consideration might also be given to the possible benefits of privacy promotion and protection in terms of fostering public support and confidence. Indeed, at a time when government accountability and transparency is a public priority, assuring Canadians that their informational privacy rights are respected might not only be good for parliamentary records management and employee/ public relations, but it could also contribute to a healthy and meaningful democracy.

(1) In 1980, the Organisation of Economic Co-operation and Development (OECD) released *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Realizing the huge potential for massive infringements of privacy from computers that could interact with one another, the OECD sought to harmonize the data protection practices of member countries by establishing some minimum standards for handling personal information. The OECD fair information practices have guided the development of privacy laws in Canada and many other countries over the last two decades.

(2) R.S.C. 1985, c. P-21.

(3) S.C. 2000, c. 5.

(4) House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, *Privacy: Where Do We Draw the Line?* April 1997, Recommendation 8.

(5) Privacy Commissioner of Canada, *Privacy Act Reform: Issue Identification and Review*, 16 June 2000, p. 127.

(6) The Charter applies to "the Parliament and government of Canada in respect of all matters within the authority of Parliament" (section 32).

(7) In *Lavigne* v. *Canada (Office of the Commissioner of Official Languages)* [2000] 214 D.L.R. (4th) 1, the Supreme Court of Canada held that the *Privacy Act* is "quasi-constitutional" legislation.

(8) [2005] 1 S.C.R. 667.

(9) Personal information generally means information about an identifiable individual, excluding the name, title or business address or phone number of an employee of an organization. Under the *Privacy Act*, for example, personal information is defined as any information about an identifiable individual, recorded in any form, including information about one's age, education, and medical or criminal or employment history (section 3).

(10) Some even contend that the Act may not fully respect the *Canadian Charter of Rights and Freedoms* (Privacy Commissioner of Canada in her appearance before the House of Commons Standing Committee on Access to Information, Privacy and Ethics, 25 October 2005).

(11) Unlike the *Privacy Act*, it is not limited to information that is recorded. Thus, it could include tissue information or blood samples.

(12) Data matching is the linking or correlating of personal data from a variety of unrelated sources, virtually always in electronic form and intended to be used for administrative purposes.

(13) Canadian Standards Association, *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96.

(14) Stephanie Perrin *et al*., *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*, Irwin Law, 2001, p. 142.

(15) Colonel Michel W. Drapeau and Marc-Aurèle Racicot, *Federal Access to Information and Privacy Legislation Annotated 2006*, Thomson Canada Limited, 2005, pp. 6-349.

(16) *Personal Information Protection and Electronic Documents Act*, Regulations Specifying Publicly Available Information, SOR/2001-7, 13 December 2000.

(17) See also the finding of the Privacy Commissioner of Canada in the case of unsolicited e-mail for marketing purposes (Summary #297), http://www.privcom/gc/ca/cf-dc/2005/297_050331_01_e.asp.

(18) Perrin (2001), p. 151.