

The Challenge of Compliance: *Privacy Protection in the Private Sector**

by Pavel Peykov

This Briefing Note describes the developments in privacy rights protection in the private sector in Canada, which culminate with the implementation of the first comprehensive piece of legislation governing commercial enterprises, the federal *Personal Information Protection and Electronic Documents Act (PIPEDA)*. This Note follows a publication by the Saskatchewan Institute of Public Policy in June 2003, which examined issues relating to privacy rights in the public sector, including the degree of individual protection from unauthorized collection, use, and disclosure of personal information. This Note attempts to present an overview of the development of privacy legislation governing the private sector in Canada and provides useful information for private businesses that manage personal information about the implementation of PIPEDA, which will soon become legally binding in all provinces and territories in Canada except Quebec.

Information technology is centrally important to the development of today's business and social environment in Canada. It has become a main force supporting economic growth and the effective provision of public services. Information technology has not only opened doors for new business and social opportunities by reducing communication and transaction costs, but it has also created challenges in regulating the flow of information among organizations and safeguarding personal integrity and entitlements against encroachment through unlawful practices in managing personal information.

The protection of individuals' privacy has become a major issue in today's knowledge-based economy, as technology has grown so rapidly that it has outpaced any attempts to develop legislative frameworks dealing with privacy rights. The first privacy laws that were in place were designed and implemented in the 1980s to regulate the management of

Saskatchewan Institute of
Public Policy
University of Regina,
College Avenue Campus
Gallery Building, 2nd Floor
Regina, Saskatchewan • S4S 0A2



General Inquiries: 306.585.5777
Fax: 306.585.5780
sipp@uregina.ca
www.uregina.ca/sipp

* The information in this article is of general and descriptive nature only. Nothing in this article is intended in any way to provide legal advice or to be relied upon as binding in a dispute, action, claim, or proceeding.

Canadian Standards Association Privacy Principles

Accountability: an organization is accountable for the personal information it has in its possession and should designate an employee or employees to oversee and enforce compliance with the applicable legislation.

Identifying Purposes: an organization should define (identify) the purposes for which personal information is to be used before or at the time of the collection of that information.

Consent: an individual must consent to the collection, use, disclosure and retention of his/her personal information except in limited circumstances. Legal, medical or security reasons may make it impossible or inappropriate to seek consent, for example, when the individual is a minor, seriously ill, or mentally incapacitated, as well as for prevention of crime or law enforcement. The prescribed form of consent depends on the type of information and the purposes for which it is to be used.

Limiting Collection: an organization should control and limit the collection of personal information to the amount necessary for the identified purposes.

Limiting Use, Disclosure, and Retention: personal information should only be used for the purposes identified by the organization, except when the individual has given his/her consent or for law enforcement. Personal information should not be retained by an organization for a period longer than necessary for the accomplishment of its intended purposes.

Accuracy: all personal information should be accurate, complete and up-to-date for the identified purposes.

Safeguards: an organization should implement adequate safeguards for the protection of personal information corresponding to the level of sensitivity of that information.

Openness: an organization is responsible for properly informing individuals about its policies and practices with regards to the management of personal information in its possession.

Individual Access: an individual should have access to his/her personal information held by an organization, upon request. There are certain exceptions, however: in instances where it is costly to provide such information, where the information refers to other individuals, or for reason of business or litigation privilege. These exceptions, on the other hand, should be limited and specific.

Challenging Compliance: an individual should have the right to challenge an organization's information security policy or practice with respect to compliance with the applicable privacy legislation.

personal information in possession of governments. In recent years, however, the private sector has increased its collection, use, and disclosure of personal information, which, in many cases, occurs without the knowledge or consent of the individual. Concern about private sector abuse of privacy has given rise to a demand that governments control (or limit) the flow of personal information managed by private and non-profit organizations. The legislative response is an attempt to balance the need to perform commercial activities using personal information with a reasonable level of protection of that information.

Privacy Standards and Existing Legislative Provisions Across Canada

In Canada, the issue of privacy rights protection has received much publicity and prompted a reaction from both public and private organizations. All provinces except Newfoundland and Labrador have already implemented privacy laws governing the public sector, while numerous industry associations and other private entities have developed their own fair-information and privacy policies. In addition, Alberta, Saskatchewan, and Manitoba have passed legislation governing the collection, use, and disclosure of personal health information. This legislation applies to all government departments, agencies, hospitals and other health-care facilities, and health professionals who are in possession of such information.

Recent attempts have been made by business and other private-sector organizations to establish

PIPEDA requires individuals and organizations covered by the Act to abide by a set of rules for managing personal information. The legislation will apply to all private and non-profit entities engaging in commercial activities that are in possession of personal information.

national standards for the management of personal information in Canada. The most influential privacy code to date has been the *Model Code for the Protection of Personal Information*, which was created by the Canadian Standards Association (CSA) and published in 1996. It contains 10 privacy principles that serve as a mechanism for evaluating an organization's privacy policy and practices. These principles are: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance. The CSA model is relevant for all types of organizations - public, private, and non-profit - because the issues of individuals' access to their own personal information and privacy rights protection are universal and independent of organizational structure and ownership. However, the privacy policies and codes adopted by private organizations throughout Canada are voluntary and not legally enforceable. They only provide instructive ethical guidelines for good business practices and do not bind individual companies to strictly adhere to them.

Privacy Legislation in the Private Sector

Effective January 1, 2004, the *Personal Information Protection and Electronic Documents Act (PIPEDA)* will govern the collection, use, disclosure, and

retention of personal information managed by all organizations engaged in commercial activities within a province or territory in Canada except Quebec. Unlike the *Model Code for the Protection of Personal Information* and other industry-adopted privacy codes and practices, PIPEDA is a law and requires individuals and organizations covered by the Act to abide by a set of rules for the management of personal information.

The intention of the federal government was that PIPEDA be implemented in three stages, over a three-year period, to allow all the parties affected to adequately prepare for compliance. The first stage began on January 1, 2001, when the legislation became applicable to all federally-regulated businesses in possession of personal information (except health information). Examples of businesses covered by the first stage include: banks, telecommunications companies, transportation companies, and airlines. The first stage also covered organizations that disclose personal information outside the boundaries of one province or the country. In its second stage, which was initiated on January 1, 2002, the legislation covered personal health information managed by the organizations affected in the first stage. The third and final stage of the implementation process will begin on January 1, 2004 when the legislation

will apply to all private entities engaging in commercial activities that are in possession of personal information. Organizations and/or activities in a province may be exempt from the force of the Act if provinces have enacted their own legislation on privacy rights in the private sector and it is “substantially similar” to PIPEDA.

Several provinces have already taken steps in that direction in order to avoid falling into the scope of the federal Act. Quebec was the first jurisdiction to pass separate legislation in 1994, even before the introduction of PIPEDA. The Quebec legislation was deemed to be substantially similar to the federal Act by the former Privacy Commissioner of Canada, George Radwanski. British Columbia has also passed legislation, *The Personal Information Protection Act*. It is not clear at this stage, however, whether businesses in British Columbia will be exempt from the application of PIPEDA. Another province, Alberta, has recently passed a similar bill in its legislature, which awaits a vote on subsequently introduced amendments. Alberta’s Bill 44 (*Alberta Personal Information Act*) is expected to take effect simultaneously with PIPEDA. Again, like British Columbia, it remains to be seen whether the Alberta legislation will be deemed to be substantially similar to PIPEDA.

A number of differences between PIPEDA and the Alberta and British Columbia Acts have been identified. The most important difference is that the

regulations established in PIPEDA are based on the principle that express consent should be required wherever possible. In PIPEDA, all personal information managed by the private sector that is collected, used, and/or disclosed must be subject to consent by the individual, except in limited circumstances. However, the legislation does not explicitly identify the types of personal information that require express and implied consent, which may create implications for both the individual and the organization that manages his/her personal information in terms of compliance. The two provincial laws specify the type of consent that is appropriate in a given situation, e.g., the management of employee information or commercial transactions, and allow the collection of employee information without consent as long as this is done for “reasonable” purposes. The federal legislation does not exempt information collected before the legislation came into force. On the other hand, the Alberta and British Columbia laws contain a grandfathering clause, which exempts organizations from seeking individual consent for information collected prior to the legislation coming into force. Another important difference between PIPEDA and the provincial acts is that PIPEDA gives the federal Privacy Commissioner power only to make recommendations while the provincial acts give more authority to their respective privacy commissioners by allowing them to issue binding orders to resolve disputes.

"Organizations and/or activities in a province may be exempt from the force of the Act if provinces have enacted their own legislation on privacy rights in the private sector and it is “substantially similar” to PIPEDA."

In 2002, Ontario submitted to stakeholders a draft proposal for privacy legislation. It was anticipated that the proposal would include provisions for the protection of personal health information, in addition to other personal information. The then federal Privacy Commissioner, George Radwanski, expressed general satisfaction with the draft, but also offered specific suggestions for strengthening the bill. The Government of Ontario, however, did not follow up on the draft proposal and it is not expected that the province will pass its legislation before PIPEDA comes into full force.

The federal Privacy Commissioner is vested with the responsibility to provide an opinion on whether a provincial privacy law is substantially similar to PIPEDA, but the Commissioner cannot legally force compliance or exempt organizations. This authority is given to the Minister of Industry Canada, who determines if provincial legislation is substantially similar to PIPEDA and submits an official recommendation to the Governor-in-Council. The Governor-in-Council has the ultimate authority to decide. The process of establishing whether provincial legislation is substantially similar was outlined in the *Canada Gazette* Part 1 on September 22, 2001. Individual provinces, territories, or organizations can present legislation to the Minister of Industry Canada that they consider substantially similar to the federal Act. While the federal Privacy Commissioner used PIPEDA to help determine if a provincial privacy law was substantially similar, the Minister could base an assessment on whether the assessed legislation reflects similar broad legislative goals. The Minister may then recommend to the Governor-in-Council that the

legislation be designated as substantially similar and exempt an organization and/or activity from the scope of PIPEDA. According to the *Canada Gazette*, the Minister of Industry will be looking for the incorporation of three elements in provincial legislation to determine whether a privacy law is substantially similar: the inclusion of the ten privacy principles from the *Model Code for the Protection of Personal Information*; the existence of provisions for independent and effective oversight, and a mechanism for investigating complaints about the protection of personal information; and the presence of restrictions on the collection, use, and disclosure of personal information to purposes that are legitimate and consistent with an organization's stated purposes for seeking such information.

What can Organizations do to Comply with PIPEDA?

There is no simple mechanism for ensuring an organization's practices meet the requirements of PIPEDA. The process of preparing for compliance does require careful attention and may consume significant resources. There are, however, a number of steps that may be considered by organizations in adapting their policies and practices to the reality of PIPEDA.

1. Organizations should establish whether they fall under the scope of PIPEDA. Some organizations and/or activities may be exempt from the Act depending on whether they are located in a province with its own substantially similar legislation to PIPEDA.

2. If an organization must comply with PIPEDA, it should estimate the cost of compliance, including the creation and maintenance of a privacy office, and the designation of employees who would deal with privacy issues.
3. Organizations should be aware of the time period necessary to become fully compliant with PIPEDA in relation to the legislation's implementation schedule.
4. There is a need to identify the types of personal information managed by an organization according to its degree of sensitivity in order to provide adequate safeguards against unlawful use or disclosure.
5. If an organization does not have a privacy policy in place, it must devise one and strictly enforce it. All employees should be educated on the organization's privacy policy.
6. Organizations should estimate the risk of mismanaging personal information and the consequences of such action. PIPEDA contains a section on remedies for non-compliance.
7. If organizations need clarification on the implications of PIPEDA, they should contact the Office of the Information and Privacy Commissioner in their province or any institution that may be knowledgeable about PIPEDA.

Saskatchewan and PIPEDA

Saskatchewan has not yet introduced legislation to protect the personal information managed by private entities operating within its boundaries. The federal Act will govern the collection, use, and disclosure of personal information within the province by default. This means that all private and non-profit organizations in the province, from small corner stores to large corporations, will have to comply with PIPEDA and be legally responsible for any breach of privacy policy. If a company collects personal information from customers, the company must show that it manages that information in a way consistent with PIPEDA. Failure to do so may result in civil action, damage to the company's reputation, customer distrust, adverse publicity, or damage to business relationships. Therefore, businesses must ensure that they not only have a privacy policy in place that is compliant with PIPEDA, but also strictly enforce it to avoid commercial and legal consequences.

The Freedom of Information and Protection of Privacy Act, which establishes the legislative framework for the collection, use, and disclosure of personal information by government departments and agencies, contains a provision to appoint an Information and Privacy Commissioner. The latter is mandated to deal with disputes regarding privacy rights, carry out research on issues within the scope of the Act, and educate the public on privacy matters. The Commissioner prepares reports with recommendations on the cases he has reviewed and gives reasons for his/her recommendations. On November 1, 2003, the first full-time Information

and Privacy Commissioner in the province, Mr. R. Gary Dickson, Q.C., took office. He will undoubtedly play an important role in matters relating to the protection of personal information, however, as long as organizations in Saskatchewan are covered by the statutes in PIPEDA, and not by provincial legislation, the scope of the Provincial Information and Privacy Commissioner's activities under PIPEDA may be limited to providing education on the content and implications of the Act. In addition, it is still unclear to what extent the federal Privacy Commissioner will be involved in privacy reviews in provinces without their own legislation for the private sector.

Conclusion

The requirement to comply with PIPEDA will undoubtedly encourage organizations to become familiar with the legislation and prepare for its implementation. However, although the deadline for compliance is approaching fast, there are few signs that organizations are in a rush to comply. The

legislation is enforced through a complaint process, which may allow some organizations to avoid – for a time - negative consequences if non-compliant privacy processes are not put in question. Being complacent, however, in the hope that no one will raise red flags about the protection of personal information is risky. Given the litigious society we live in, it seems clear that, with the implementation of PIPEDA, people will become more attentive to whether their privacy rights are being respected. The risk of complaints under PIPEDA, civil action, and loss of reputation is real. Organizations must work to identify and manage this risk by becoming aware of the requirements of PIPEDA and the consequences of non-compliance, establishing an internal process of dealing with privacy issues, and ensuring that all personal information collected, used, and disclosed is adequately protected. At this stage, the questions and inquiries about the impact of PIPEDA on organizations and activities outnumber the answers by a significant margin. However, it is hoped that through a process of extensive public education and interaction among different stakeholders, organizations will be able to prepare for compliance more effectively.

Our Author: Pavel Peykov, SIPP Policy Analyst

Pavel Peykov joined the Institute during the summer of 2002. He was previously employed with Saskatchewan Energy and Mines and the University of Regina. Mr. Peykov's education includes a Bachelor of Arts (Honours) in Business Administration from the University in North London, London, England and a Master of Arts in Economics from the University of Regina. He is currently working towards a Master of Public Administration from the University of Regina. For more information, please call Pavel at (306) 585-5862.

Previous SIPP Publications by Pavel Peykov include: Public Policy Paper 18, *Labour Issues in the Provision of Essential Services*; Briefing Note 2, *Information Management and Privacy Rights: Are We Adequately Protected Against Intrusion in Our Lives?*; and Briefing Note 1: *Choice in Automobile Insurance: Tort vs. No Fault Coverage* (Revised).

The Saskatchewan Institute of Public Policy

Saskatchewan Institute of Public Policy
University of Regina, College Avenue Campus
Gallery Building, 2nd Floor
Regina, Saskatchewan • S4S 0A2



General Inquiries: 306.585.5777
Fax: 306.585.5780
sipp@uregina.ca
www.uregina.ca/sipp

www.uregina.ca/sipp

The Saskatchewan Institute of Public Policy (SIPP) was created in 1998 as a partnership between the University of Regina, the University of Saskatchewan and the Government of Saskatchewan. It is, however, constituted as an institute at the University of Regina. It is committed to expanding knowledge and understanding of the public-policy concerns in Canada with a particular focus on Saskatchewan and Western Canada generally. It is a non-profit, independent, and non-partisan Institute devoted to stimulating public-policy debate and providing expertise, experience, research and analysis on social, economic, fiscal, environmental, educational, and administrative issues related to public policy.

The Institute will assist governments and private business by supporting and encouraging the exchange of ideas and the creation of practical solutions to contemporary policy challenges. The Founding Partners intended the Institute to have considerable flexibility in its programming, research, contracting and administration so as to maximize opportunities for collaboration among scholars in universities and interested parties in the public and private sectors.

The Institute is overseen by a Board of Directors drawn from leading members of the public, private and academic community. The Board is a source of guidance and support for SIPP's goals in addition to serving a managerial and advisory role. It assists SIPP with fostering partnerships with non-governmental organizations, the private sector and the expanding third sector.

Saskatchewan enjoys a long and successful tradition of building its own solutions to the challenges faced by the province's citizens. In keeping with this tradition, the Saskatchewan Institute of Public Policy will, in concert with scholars and practitioners of public policy, bring the best of the new ideas to the people of Saskatchewan.

THE SIPP BRIEFING NOTE

The SIPP Briefing Note series allows the Institute to review and comment on public-policy issues that affect the people of our community. A SIPP Briefing Note will be released several times a year and can be used as an instrument for further discussion and debate.

OCTOBER 2003 - Filling the Empty Vessel: Defining the Mandate and Structure of a Council of the Federation

SEPTEMBER 2003 - The Art of the Possible: The Interpersonal Dimension of Policy-Making in the Case of the Northern Development Accord

JUNE 2003 - Information Management and Privacy Rights: Are we Adequately Protected Against Intrusion in Our Lives?

DECEMBER 2002 - Choice in Automobile Insurance: Tort vs. No Fault Coverage



UNIVERSITY OF
REGINA