FASKEN MARTINEAU

CANADIAN PRIVACY LAWS: COUNTDOWN TO JANUARY 1, 2004

By Sara A. Levine and J. Alexis Kerr, Fasken Martineau DuMoulin LLP

On January 1, 2004, new data protection legislation will enter into force in Canada, changing the regulatory landscape for every organization in Canada that collects, uses or discloses personal information in the course of commercial activity. Organizations operating in Canada should take note of the new obligations and must begin preparations now in order to ensure that they are compliant by the end of 2003. Organizations that fail to do so may well find their privacy practices under scrutiny by a Privacy Commissioner or by members of the public, risking both legal liability and harm to their brand and goodwill.

Background

Over the past 10 years there has been an explosive growth worldwide in public concern over and government regulation of the privacy of personal information. In particular, the federal governments in both Canada and the United States have significantly increased their oversight of the private sector's collection, use and disclosure of personal information. Although these changes were prompted in part by the data protection regime existing in the European Union, the Canadian government took a very different approach to personal data protection than that taken by the U.S.

In 1995, the European Commission promulgated the *Directive on the Protection of Individuals in Relation to the Processing of Personal Data* ("EC Directive").[1] The EC Directive established rules applying to the collection, use, disclosure, retention and destruction of personal data. It also imposed restrictions on transborder data flows of personal data to jurisdictions without equivalent

[1] 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 (October 24, 1995), Article 25 and 26, **online: European Commission Homepage <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett> (last accessed: September 11, 2003)** [hereinafter "Directive"].**]**

standards, effectively creating a non-tariff barrier to trade. In response, the Canadian government enacted the *Personal Information Protection and Electronic Documents Act* (the "PIPEDA").[2]

Generally applicable at present only to federal works, undertakings and businesses (and to organizations operating in Canada's three Territories), the PIPEDA regulates organizations in the private sector that collect, use or disclose personal information about an identifiable individual in the course of commercial activity. From and after January 1, 2004, it will apply throughout Canada unless a province enacts "substantially similar", in which case the provincial legislation may trump the PIPEDA in certain circumstances.

There is existing or proposed privacy legislation in several provinces. In Quebec, the *Act Respecting the Protection of Personal Information in the Private Sector* (the "Quebec Act") will generally apply within that province.[3] There are also provisions relevant to the privacy of personal information in the *Civil Code of Quebec* and in the *Quebec Charter of Human Rights and Freedoms*. British Columbia and Alberta have introduced omnibus Bills to protect personal information,[4] which are expected to be enacted shortly and to enter into force on or before January 1, 2004. Alberta also has health privacy legislation in force,[5] as do Saskatchewan and Manitoba, however this health sector specific legislation is not addressed in this paper.[6] None of the other provinces currently have private sector privacy laws, although Ontario has made at least two attempts at drafting its own legislation.

Canadian Privacy Laws Differ From American Privacy Regimes

By contrast, the U.S., having historically taken a market-based, sectoral approach to privacy regulation,[7] has sought to avoid enacting omnibus federal legislation. In June 2000, the U.S.

---

2 S.C. 2000 c.5

3 RSQ 1982 c.A-2.1 as am.

4 Bill 38 and Bill 44 respectively, which are each entitled the *Personal Information Protection Act*.

5 R.S.A. 2000, c.H-5

6 SS. 1999, c.H-0.021; and S.M. 1997, c.51

7 The sectoral approach to privacy regulation has resulted in an increasing number of privacy laws at the state and federal level in the United States. The sectors affected include financial services (e.g. the *Gramm-Leach-Bliley Act*), credit reporting agencies (e.g. the *Fair Credit and Reporting Act*), telemarketing, health (e.g. the *Health*

Department of Commerce and the European Commission negotiated a compromise between the self-regulatory approach of the U.S. and the legislative approach of the EU. The compromise is known as a "Safe Harbor" arrangement.

The Safe Harbor is a voluntary, primarily self-regulatory system. Under the Safe Harbor, an American company may voluntarily agree to adhere to the personal information rules agreed to by the U.S. and the EU as being adequate in light of the EC Directive. Once an organization has joined the Safe Harbor it must adopt various measures that are consistent with the seven Safe Harbor principles to ensure that data is adequately protected.[8] Organizations may qualify for the Safe Harbor by either self-certifying compliance or by obtaining third party verification. The Safe Harbor principles are less onerous than the obligations (particularly the administrative obligations) imposed on organizations operating in Canada by the PIPEDA and proposed and existing provincial privacy laws.

The PIPEDA and Omnibus Provincial Privacy Laws

Definitions

Personal information is generally defined in these omnibus data protection statutes to include all information about an identifiable individual, except (in the case of the PIPEDA) the name, title, business address and business telephone number of an employee of an organization. An individual's name need not be attached to the information in order for it to qualify as personal information: if the information can be 'linked' with identifying information, it will qualify as "personal". The term "organization" includes an association, a partnership, a trade union and a person (including a corporation).

Information Portability and Accountability Act) and education. The subject-specific legislation includes state and federal laws relating to mailing lists, employment records, electronic surveillance (including telephone and video recording and the use of global positioning systems), children's websites (e.g. the *Children's Online Privacy Protection Act*), and the use of Social Security numbers. In addition, many other statutes at both the federal and state levels contain provisions addressing privacy issues. This patchwork has resulted in a complex and confusing privacy landscape in the United States.

[8] The seven principles of the Safe Harbor are: Notice, Choice, Onward Transfer, Access, Security, Data Integrity, and Enforcement.

The Consent Requirement

The PIPEDA establishes rules that require all private sector organizations operating in Canada that collect, use or disclose personal information in the course of commercial activity to obtain an individual's prior informed consent to such collection, use and disclosure, subject to certain enumerated exceptions. The informed consent requirement obliges the organization to identify to the individual the purposes for the use and disclosure of the personal information collected (and the types of parties to whom the personal information is disclosed). The organization is generally limited to using and disclosing the information only for the identified purposes, and to disclosing the information only to the identified (types of) parties.

In Quebec, upon establishing a file, an enterprise must inform the data subject of: the object of the file, the use that will be made of the file, the categories of persons within the enterprise that will have access to the file, the place where the file will be kept and the data subject's rights of access and rectification. An "enterprise" is defined in the *Civil Code of Quebec* as "the carrying on by one or more persons of an organized activity, whether or not it is commercial in nature, consisting of producing, administering or alienating property, or providing a service".

The PIPEDA provides that express consent is the highest form of consent, but also contemplates reliance on implied consent, depending on the sensitivity of the information. In Quebec, the consent to use or disclosure is valid only if it is free, enlightened, manifest and given for a specific purpose; it is also time-limited. "Implicit" consent is considered valid in Quebec only in relation to the use and communication of a nominative list (a list of names, addresses and telephone numbers of natural persons) for the purpose of commercial or philanthropic prospection. The British Columbia and Alberta Bills permit reliance on deemed consent in certain circumstances. In obtaining or relying on any such forms of consent as described above, however, the reasonable expectations of the individual are relevant.

Individuals may withdraw their consent on reasonable notice, at any time, subject to contractual limitations.

Application

As stated above, the PIPEDA applies to collections, uses and disclosures of personal information by organizations that occur in the course of commercial activity. The scope of the "commercial activity" requirement is the subject of much debate and remains to be judicially considered.

The British Columbia and Alberta Bills do not impose a "commercial activity" requirement, such that they will apply to all organizations within those provinces that collect, use and disclose personal information. In addition, they provide that organizations may collect, use and disclose personal information about their own employees without the employees' consent, provided such collection, use or disclosure is for the purposes of establishing, managing or terminating an employment relationship with the organization. It remains to be seen how these provisions will be interpreted and applied.

The Quebec Act applies to personal information that a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise in Quebec. When engaging in any of those activities, an enterprise must have a serious and legitimate interest in establishing a file on another person, must stipulate the object of the file, and must collect, use, handle or disclose only the information required to fulfil the object of the file. Enterprises must collect the information directly from the data subject unless the individual consents to collection from a third party, subject to limited exceptions. The source of the information must be included in the file.

Grandfathering

There is no 'grandfathering' provision in the PIPEDA to exempt organizations from its application to the collection, use or disclosure of information already in their possession. Under the PIPEDA, therefore, an organization will be unable to use or disclose any personal information that it collected prior to that date without the prior knowledge and consent of the individual concerned, unless one of the limited exceptions applies.

Conversely, the proposed provincial legislation Alberta and British Columbia contain limited 'grandfathering' provisions that are applicable in certain circumstances.

Administrative Requirements

All of the data protection legislation in Canada imposes obligations on organizations to establish policies and implement practices concerning the handling of personal information, as well as various logistical and administrative obligations. Organizations are responsible for the personal information under their control and must designate an individual who is accountable within the organization for the organization's compliance with the legislation. Organizations are also responsible for the information handling practices of their agents and of entities that process information on their behalf, and must contractually bind such entities or individuals to ensure a comparable level of protection.

In addition, all of the protection legislation in Canada requires organizations to protect the information with security safeguards, which includes physical, organizational and technological measures, as needed. Organizations are generally required to guard against external threats, but also against unauthorized internal use, access, disclosure, copying, or modification. These security obligations apply regardless of the format in which the information is held. Communications by an organization to an individual in respect of the individual's personal information (including but not limited to email communications) will also be generally subject to the same security obligations. Such communications should be made in a manner that ensures that the security of the information will be maintained in the course of the communication (for instance, secure email encryption, letter-mail envelopes with no outside identifiers or clear plastic "windows", no inappropriate use of "call display" technology).

Access by employees of the organization to personal information should be limited to those employees who need to know the personal information to carry out a legitimate identified purpose for which the organization has consent (either express, implied or deemed, as the case may be).

Organizations must ensure that the personal information is as accurate, complete and up to date as necessary for the identified purpose, but may not routinely update the information unless it is necessary to fulfill that purpose. Organizations may generally retain information only for as long as is necessary to fulfill the identified purpose, and should develop and implement retention policies specifying minimum and maximum retention periods. Information that is no longer

required must be destroyed, erased or made anonymous, and organizations should have policies and procedures regarding destruction to ensure that the security of information is maintained in the course of destruction.

The Individual's Rights

Individuals are granted the right, upon written request, to access their own personal information held by an organization, and to be informed of the identities of the parties to whom the information has been disclosed, subject to certain limited exceptions. They also have a right to request that the information be amended, deleted or corrected. An organization must generally respond to such requests within the time period prescribed by the relevant statute. While an organization has limited rights to refuse to amend, delete, correct or provide access to such information, it may be required to give reasons for such refusal. Where an organization amends or corrects an individual's personal information, it should advise third parties to whom the information has been disclosed of the amendment or correction.

Generally, organizations must make readily available to individuals specific information about their policies and practices in respect of their management of personal information. The information must be made available in a form that is generally understandable and must include certain types of information as specified in the respective statutes (including but not limited to the name or title of the accountable person, the access procedure and the organizations to which the personal information may be disclosed). Individuals may also challenge the organization's compliance with their obligations, and organizations must have a complaints procedure in place to receive and respond to such challenges.

In addition, individuals have a right to complain to the Privacy Commissioner charged with enforcement of the particular statute in the respective jurisdiction, and a right to apply to the Court for a hearing. Under the PIPEDA, complaints to the Privacy Commissioner of Canada may be made anonymously and, under some of the statutes, the complainant is not required to have a personal interest in the substance of the complaint. Thus, policy advocates, disgruntled employees and vicious competitors are equally as able to complain as those individuals whose personal information is at issue.

Powers of the Commissioners

Although the Privacy Commissioner of Canada does not have order making powers, he may: (i) publicize an organization's breaches if he feels it would be in the public interest; (ii) make recommendations respecting the policies or practices of an organization; (iii) request that the organization publish a notice of any action taken or proposed to be taken to correct such policies or practices; or (iv) include the audit report for the organization in his annual report to Parliament. The Federal Court may order an organization to comply with the obligations imposed by the PIPEDA, impose fines in limited circumstances, including fines on directors, officers and employees, and award damages for humiliation.

The Quebec Act provides that any interested person may make a written request to the Commission d'accès à l'information for examination of a disagreement concerning any provision of the Act. The Commission has all the powers necessary for the exercise of its jurisdiction and may make any order it considers appropriate to protect the rights of the parties, including rule on any issue of fact or law. Commission decisions may be filed with the Quebec Superior Court, making them enforceable as judgments of that Court.

The proposed provincial legislation in British Columbia and Alberta grants the respective provincial Commissioners broad investigatory, adjudicative and order-making powers, in addition to granting those Commissioners a public interest, educative and advocacy function. Decisions of those Commissioners may, however, be subject to judicial review.

Types of Activities involving Collection, Use or Disclosure of Personal Information

An organization collects, uses or discloses personal information if, among other activities, it:

- collects, uses, trades or sells information regarding customer preferences for marketing purposes;

- uses a customer relationship management database;

- it is involved in a corporate transaction involving the disclosure to another party of customer lists, client information, consumer profiles, membership data, or any information about a customer, client, member, donor, director, shareholder and in certain circumstances, employees;

- it uses direct marketing tools;

- it uses customer credit information;

- it engages in e-commerce; or

- it has or it generates any financial, health, consumer, religious, charitable, marketing or lifestyle information about an individual.

The Obligations – More Than a Privacy Code

The Privacy Commissioner of Canada cautioned the private sector in his most recent annual report to Parliament on January 29, 2003, that having a privacy code is pointless if an organization fails to reinforce that code with comprehensive and detailed policies and practices. These policies and practices must be implemented throughout the organization, and must be consistently observed and applied.

He also observed that the privacy violations that give rise to complaints to his office are often attributable to problems or defects in an organization's information-handling processes or administrative system as a whole. These problems often result from an organization's failure to properly understand the obligations imposed by the PIPEDA, or by the organization's continued reliance on traditional information management practices that may no longer be acceptable under the PIPEDA.

What Should Organizations Do to Become Compliant?

Organizations should conduct a detailed assessment of their existing practices with respect to their collection, use and disclosure of personal information, including the purposes for which that information is collected, used and disclosed. Organizations must then establish and implement

codes, policies and procedures throughout their organization. The impetus for privacy compliance must come from the top. Any attempt to establish new systems will fail if those assigned the task are lower-level employees.

Sara Levine is a member of the Litigation Department at Fasken Martineau DuMoulin. The Director of Firm Privacy Compliance for the Toronto Office of Fasken Martineau, she is responsible for the oversight and implementation of the Privacy Compliance Program. She is Vice-Chair of the Privacy and Information Protection Practice Group and advises clients on privacy matters generally and on matters involving the privacy of personal health information.

Alexis Kerr is a member of the Litigation Department of Fasken Martineau DuMoulin and a member of the Privacy and Information Protection Practice Group. She has extensive experience advising clients on all aspects of privacy compliance in Canada and has written widely in the area.

For more information about the Privacy and Information Protection Practice Group of Fasken Martineau DuMoulin, go to **www.fasken.com** *or call Sara Levine or Alexis Kerr at 416-366-8381.*