STIKEMAN ELLIOTT

Privacy

Section O of Stikeman Elliott's *Doing Business in Canada*

STIKEMAN ELLIOTT LLP

Privacy

Contents

General 2
PIPEDA 2
  Background 2
  General 3
  Application 3
  Obligations under PIPEDA 4
  Remedies 6
Provincial Legislation 6
  Quebec 6
  Common Law Provinces 7
  Comparing PIPEDA and the Provincial Privacy Laws 7
Health Privacy Legislation 8

© STIKEMAN ELLIOTT LLP   SEPTEMBER 2007

Privacy

GENERAL

Privacy laws regulating the collection, use and disclosure of personal information in the public sector have been in place since 1977 when the federal government passed the *Canadian Human Rights Act* (CHRA). Certain sections of the CHRA that dealt with the protection of personal information were repealed in 1983 and replaced by the federal *Privacy Act,* which today continues to apply to the collection, use and disclosure of personal information by federal government institutions. In addition, there are a variety of statutes that regulate the protection and access of personal information held by provincial and territorial government departments and agencies. In Ontario, for example, the *Freedom of Information and Protection of Privacy Act* and *Municipal Freedom of Information and Protection of Privacy Act* together legislate on the collection, use, retention and disclosure of personal information by government bodies.

The regulation of personal information in the private sector context, on the other hand, was a much later development in Canada. The impetus for the introduction of legislation regulating personal information in Canada is partially attributable to the growth of the Internet and the introduction of other technological advances which greatly facilitate the collection, retention, organization and dissemination of personal information, and partially attributable to the introduction of the European Union's "Privacy Directive" in 1995. At the provincial level, three provinces – Quebec, British Columbia and Alberta – have now passed legislation dealing generally with the protection of personal information in the private sector. Further, four provinces – Ontario, Manitoba, Saskatchewan and Alberta – have statutes that specifically address the privacy of personal health information in the private sector. At the federal level, Parliament has enacted the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which took effect on January 1, 2004 and is discussed below.

PIPEDA

Background

The Canadian government looked largely to the private sector for assistance in the creation of privacy legislation. The Canadian Standards Association had previously engaged industry, consumers, and government in a collaborative effort to create the *Model Code for the Protection of Personal Information*, which was designed to afford consumers some protection in their dealings with the private sector. The code was strictly voluntary, however, and there was no ability to enforce its provisions, or to

encourage appropriate data management within Canada. To create the appropriate regulatory environment, the government essentially took the voluntary code that had been in place, and formalized the measures into Part I of PIPEDA.

General

PIPEDA was brought into effect in three phases. The first implementation phase came into force on January 1, 2001, at which point the statute applied to the federally regulated private sector and to information disclosed for consideration across national or provincial borders. Federally regulated sectors include industries such as banking, airlines, broadcasters, shippers and telecommunications companies.

On January 1, 2002, PIPEDA was extended to apply to "personal health information" which includes any information concerning the physical or mental health of an individual (living or deceased), any health services provided to an individual, information about donations of body parts or substances, or any information collected in the course of, or incidentally to, the provision of health services to the individual.

The third and final implementation phase took place on January 1, 2004. Effective that date, PIPEDA applied to all personal information collected, used or disclosed in whole or in part within Canada in the course of "commercial activities" – defined as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering, or leasing of donor membership or fundraising lists". This final phase expanded the application of PIPEDA's privacy protections to all commercial transactions in Canada.

The Supreme Court of Canada has defined information privacy as being the right of the individual to determine when, how, and to what extent he or she will release personal information. Part I of PIPEDA provides legislative recognition of this right by giving individuals the ability to determine how an organization may use their personal information in the course of commercial activities. PIPEDA regulates the collection, use or disclosure of personal information, such as an individual's addresses, telephone numbers, email addresses, credit card information, social insurance numbers, financial information, health information, as well as consumer-specific spending history or personal habits. The legislation applies irrespective of whether the personal information was obtained directly from a consumer or indirectly from a third party.

Application

Canada has a federal structure with constitutionally defined areas of jurisdiction for the federal government and for the respective provincial governments across the country. Section 92 of the *Constitution Act, 1867* gives the provincial governments in Canada exclusive jurisdiction over local

trade, property and civil rights. Recognizing this division of powers, PIPEDA allows the federal cabinet to exempt businesses from the application of PIPEDA in a province that enacts privacy legislation found to be "substantially similar" to Part I of PIPEDA. Any such exemption applies only to collection, use, or disclosure of personal information that occurs within the province. Extra-provincial or international aspects of data collection or usage continue to be subject to PIPEDA notwithstanding such an exemption order.

PIPEDA therefore applies in respect of personal information which is collected, used or disclosed in the course of commercial activities by federally regulated private sector organizations, and personal information which is collected, used or disclosed by other private sector organizations in the course of their commercial activities when it is transferred across Canadian or provincial borders or when it is collected, used or disclosed within a Canadian province that has not enacted legislation which is "substantially similar" to PIPEDA. To date, the federal government has recognized each of the Alberta *Personal Information Protection Act* (APIPA), British Columbia *Personal Information Protection Act* (BCPIPA) and Quebec's *Act respecting the protection of personal information in the private sector* (Quebec Private Sector Act) to be "substantially similar" to PIPEDA. The *Personal Health Information Protection Act* (PHIPA) in Ontario has been found to be "substantially similar" only in regards to personal health information and so PIPEDA continues to apply in Ontario with respect to all other personal information. PIPEDA regulates the collection, disclosure and use of personal information in the private sector in all other provinces.

With respect to personal information of employees, PIPEDA only governs the collection, use, and disclosure of those persons employed by federal works or undertakings (i.e. employers in areas such as aviation, telecommunications, broadcasting and banking). Consequently, even if employee information is transferred across provincial borders, PIPEDA will not apply unless the business is federally regulated. APIPA, BCPIPA and the Quebec Private Sector Act regulate personal information of employees in the private sector (including volunteers in some cases) in those provinces.

Obligations under PIPEDA

Under PIPEDA, individuals must be provided with the ability to exercise informed consent to the collection, use, or disclosure of their personal information. PIPEDA establishes rules governing the collection, use, and disclosure of personal information, and requires organizations to establish and enforce formal policies regarding the handling of personal data. Policies must strive to respect an individual's privacy rights, while permitting the valid gathering and use of personal information by organizations. Generally, PIPEDA requires organizations to comply with

the following ten privacy principles set out in Schedule I of PIPEDA, originally set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information*:

- **Accountability:** Each organization is responsible for the personal information it collects and is required to appoint an individual who is accountable for the organization's compliance with the ten PIPEDA principles. Each organization must protect personal information it provides to third party service providers using contractual and other protections (such as encrypting personal information or providing anonymous information where possible), and must implement internal privacy policies and practices with respect to personal information in its control. Audit and compliance mechanisms should be implemented and regularly reviewed to ensure that they reflect the organization's evolving requirements.
- **Identifying Purpose:** The purpose for which personal information is collected must be identified at or before the time it is collected.
- **Consent:** Knowledge and consent are required for the collection, use and disclosure of personal information. Consent may be express or implied. Each organization must ensure that the individuals whose personal information is collected know of the purpose for which it is being collected, used or disclosed.
- **Limiting Collection:** The collection of personal information shall be limited to what is necessary in accordance with the identified purposes. There must be a clear link between the personal information collected and the identified purposes. Procedures must be developed to ensure that personal information which has already been collected is not used or disclosed for a purpose that has not been identified to the subject individual without first obtaining consent to use it for the new purpose.
- **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 and shall be retained only as long as necessary for the identified purposes.
- **Accuracy:** Personal information must be accurate, complete and current as is necessary for the identified purpose.
- **Safeguards:** Personal information must be securely protected from unauthorized access. Employees must be advised of the need to maintain the confidentiality of the personal information.
- **Openness:** Organizations must be transparent and open about their management of personal information.
- **Individual Access:** On request, individuals must be provided with access to and the ability to correct their personal information, and a list of third parties to whom such information has been disclosed must be made available on request.

- **Challenging Compliance:** Individuals should be able to challenge an organization's compliance with privacy principles. Each organization must implement procedures to receive and respond to complaints or inquiries about its policies and practices with respect to personal information.

Remedies

Individuals have the right to complain to the Privacy Commissioner of Canada or, in certain circumstances, to the courts. PIPEDA gives the Privacy Commissioner of Canada broad investigative and audit powers to resolve disputes and establish effective systems of compliance. In addition, the Privacy Commissioner has the ability to publicly disclose all information relating to the personal information management practices of an organization if it considers such disclosure in the public's interest. The legislation also provides "whistle blowing" protections for employees who report violations, provided the reports are made in good faith or upon reasonable belief.

If an organization fails to comply with PIPEDA, it may be ordered to correct its practices and to publish a notice of such action. Damages may be awarded to the complainant, including damages for humiliation. In addition, failure to comply with certain provisions of PIPEDA may result in an organization, director, officer or employee being fined up to $100,000.

PROVINCIAL LEGISLATION

As mentioned above, currently only Quebec, British Columbia and Alberta have enacted general private sector privacy legislation and each these provincial enactments has been recognized as being "substantially similar" to PIPEDA. Privacy protection legislation varies significantly from province to province, and despite the requirement that the provincial legislation be "substantially similar" to PIPEDA, certain protections are nonetheless available in some provinces while not in others.

Quebec

The Quebec Private Sector Act regulates the collection, storage, and communication of personal information about individuals by private enterprises operating in the province. The rules established by the Quebec Private Sector Act serve to supplement the privacy provisions contained in Quebec's *Civil Code*, and also address issues respecting the transfer of personal information outside of the province.

In 2003, the federal government recognized the Quebec Private Sector Act to be "substantially similar" to Part I of PIPEDA and therefore most non-federally regulated businesses operating in Quebec are exempt from that part of the federal legislation dealing with personal information. Accordingly, the Quebec legislation will apply within the province of

Quebec to the exclusion of PIPEDA, as long as all of the actions of the commercial enterprise occur within the province. Where the collection, use or disclosure of personal information occurs across Quebec's borders, conceivably both PIPEDA and the Quebec Private Sector Act could apply.

Common Law Provinces

Currently, only PIPEDA regulates personal information practices in the Ontario private sector. In February 2002, the provincial Ministry of Consumer and Business Services released draft legislation entitled the *Privacy of Personal Information Act, 2002*, which was to serve as the foundation for Ontario's private sector privacy legislation, but in the end no bill based on the draft legislation emerged. In October 2003, British Columbia passed the BCPIPA governing the collection, use and disclosure of personal information by organizations in the province. Alberta followed suite, passing its APIPA in December 2003. Both the British Columbia and Alberta PIPAs came into force on January 1, 2004 and were declared substantially similar on October 12, 2004.

Comparing PIPEDA and the Provincial Privacy Laws

When comparing PIPEDA and the provincial privacy legislation, one matter that needs to be highlighted is the issue of consent. PIPEDA requires express ("opt-in") consent when the personal information collected, used or disclosed is sensitive (such as in the case of a person's health or financial information). Implied ("opt-out") consent is permissible under PIPEDA where the personal information is not sensitive (e.g. a person's mailing address in the case of a mainstream magazine subscription). Both the BCPIPA and APIPA, on the other hand, allow for implied consent for all types of personal information provided certain reasonableness criteria are met. In Quebec, consent must be manifest, free and enlightened, and must be given for a specific purpose.

Another issue that is of importance when comparing federal and provincial private sector privacy law has to do with the purchase or sale of a business. Both the BCPIPA and APIPA have an exemption from the consent requirement for the collection, use and disclosure of personal information by an organization in the course of a "business transaction" which by definition includes a purchase, sale or lease, merger or amalgamation involving that organization. In Quebec, on the sale or purchase of a business, the consent of the relevant customers as well as employees will be required before any personal information may be disclosed to potential purchasers. In contrast, there is no equivalent "business transaction" exemption under PIPEDA (although the issue was raised in the recent five-year review of PIPEDA and is slated to change). Accordingly, it would be prudent to obtain consent of the relevant individuals prior to transferring any personal information in a business transaction context if the federal legislation is applicable.

HEALTH PRIVACY LEGISLATION

There are a multitude of laws that apply to the privacy of personal health information in the private sector. PIPEDA applies to the collection, use and disclosure of personal health information generally, and four provinces – Ontario, Alberta, Saskatchewan and Manitoba – have enacted specific legislation concerning personal health information.

Since Ontario's *Personal Health Information Protection Act, 2004* has been deemed to be "substantially similar" to PIPEDA with respect to personal health information, PIPEDA does not apply in Ontario to that extent. Persons dealing with personal health information in Saskatchewan and Manitoba, the PHIPAs of which have not yet been declared "substantially similar" with PIPEDA, must comply both with their respective provincial statute, and with PIPEDA. The situation in Alberta is unclear: while the general provincial private sector privacy legislation has been deemed to be substantially similar to PIPEDA, the health sector specific statute has not and so PIPEDA could still possibly apply to certain personal health information issues. In B.C. and Quebec, the legislation governing personal information in the private sector also covers personal health information; therefore PIPEDA presumably does not apply in those two provinces. PIPEDA continues to govern in all provinces where personal health information crosses provincial or national borders.

Canadian Business Law – Worldwide

Stikeman Elliott is recognized nationally and internationally for the sophistication of its business law practice. The firm is a Canadian leader in each of its core practice areas – corporate finance, M&A, securities, banking, corporate-commercial, real estate, tax, insolvency, structured finance, competition, intellectual property, employment and business litigation – and has developed in-depth knowledge of a wide range of industries.

Chambers Global identifies the firm as one of Canada's two top-tier Corporate/M&A practices and it is frequently ranked among Canada's leaders in domestic and cross-border M&A league tables from Thomson Financial, Mergermarket and Mergerstat Review. Stikeman Elliott is also the leading adviser in Canadian securities offerings, ranking first from 2005 to 2009 (inclusive) in Bloomberg league tables in terms of overall volume, as well as receiving top rankings from the *Financial Post*. The firm's National Litigation Group, whose specializations include class actions, securities litigation and restructurings, has been ranked among the top three business litigation practices in Canada by Lexpert. Among Stikeman Elliott's other highly regarded practices are competition/antitrust (named as a leader by the *Global Competition Review*), taxation (highly ranked by Lexpert) and structured finance (widely considered to be Canada's foremost practice in that field).

The firm's clients can expect a consistently high level of service from each of its eight offices who work together on major transactions and litigation files, and regularly collaborate with prominent U.S. and international law firms on cross-border transactions of global significance. The firm has invested heavily in leading-edge knowledge management systems in order to assure our clients of advice of the highest quality, grounded in the accumulated expertise of Stikeman Elliott's national and international practice.

STIKEMAN ELLIOTT

MONTRÉAL TORONTO OTTAWA CALGARY VANCOUVER NEW YORK LONDON SYDNEY

www.stikeman.com

This publication is intended to provide general information about developments in the law and does not constitute legal advice.

For further information please contact your Stikeman Elliott representative or any of the Managing Partners or Principals listed below:

MONTRÉAL
1155 René-Lévesque Blvd. West, 40th Floor, Montréal, QC, Canada H3B 3V2
Tel: (514) 397-3000 Fax: (514) 397-3222
Contact: André J. Roy aroy@stikeman.com

TORONTO
5300 Commerce Court West, 199 Bay Street, Toronto, ON, Canada M5L 1B9
Tel: (416) 869-5500 Fax: (416) 947-0866
Contact: Roderick F. Barrett rbarrett@stikeman.com

OTTAWA
Suite 1600, 50 O'Connor Street, Ottawa, ON, Canada K1P 6L2
Tel: (613) 234-4555 Fax: (613) 230-8877
Contact: Stuart McCormack smccormack@stikeman.com

CALGARY
4300 Bankers Hall West, 888 - 3rd Street S.W., Calgary, AB, Canada T2P 5C5
Tel: (403) 266-9000 Fax: (403) 266-9034
Contact: G. Frederick Erickson ferickson@stikeman.com

VANCOUVER
Suite 1700, Park Place, 666 Burrard Street, Vancouver, BC, Canada V6C 2X8
Tel: (604) 631-1300 Fax: (604) 681-1825
Contact: Ross A. MacDonald rmacdonald@stikeman.com

NEW YORK
445 Park Avenue, 7th Floor, New York, NY 10022
Tel: (212) 371-8855 Fax: (212) 371-7087
Contact: Kenneth G. Ottenbreit kottenbreit@stikeman.com

LONDON
Dauntsey House, 4B Frederick's Place, London EC2R 8AB England
Tel: 44 20 7367 0150 Fax: 44 20 7367 0160
Contact: Derek N. Linfield dlinfield@stikeman.com

SYDNEY
Level 12, The Chifley Tower, 2 Chifley Square, Sydney N.S.W. 2000 Australia
Tel: (61-2) 9232 7199 Fax: (61-2) 9232 6908
Contact: Brian G. Hansen bhansen@stikeman.com