

Privacy Legislation for Canada's Private Sector

Understanding Canada's *Personal Information Protection and Electronic Documents Act*. September, 2003.

Purpose

For many years, privacy legislation in Canada concerned the government's use, storage and dissemination of personal information. With the passage of the Personal Information Protection and Electronic Documents Act (herein 'PIPEDA' or 'Act'), businesses throughout Canada will now see their collection, retention and dissemination of personal information directed by legislative demands. The spirit of PIPEDA is echoed in s.3 of the Act, which seeks to balance the competing interests of maintaining the privacy of personal information, while respecting the need for commercial organizations to reasonably collect and use such information. The Act emanates from the Canadian Standards Association's Model Code for the Protection of Personal Information, originally a voluntary code, which was wholly incorporated into the Schedule 1 of the Act. Section 5(1) of the Act makes Schedule 1 binding legislation.

Personal Information

The major purpose of the *Act* is the protection of personal information, meaning, any information about an identifiable individual, including clients and employees, that relates to his or her personal characteristics, (i.e. gender, colour, age, ethnicity, education) their health, activities and views (i.e. religion, purchasing patterns or opinions). s.2(1) The *Act* apparently does not protect corporate information, meaning, the information a business collects about a corporate client is beyond the scope of the *Act*.

For an employer, personal information retained about an employee may include a social insurance number, medical records required for hiring purposes, the results of appropriately conducted drug testing, and driver's licence particulars.

For a business entity, personal information collected about a customer may include detailed banking information, personal finances, spending habits, gender, and education.

Who Does PIPEDA Apply To? (s.4)

Phase 1: Federal Works

Currently, the *Act* applies to all personal information, including personal health information that is collected, used, or disclosed in the course of commercial or employment activities, by a federal work. Companies traditionally deemed a federal work come under federal jurisdiction, and include banks, airlines, telecommunications, broadcasters and transportation companies. By operation of s.4(1)(b) of the *Act*, a federal

employer must also apply the *Act*'s provisions to their employer - employee relationships. The *Act* also applies to provincially-regulated organizations when they are sold, leased, or bartered across provincial or national boundaries. The mere fact that a company is federally incorporated does not automatically mean that corporation is a federal work. Companies subject to any part of the *Canada Labour Code* are likely a federal work.

Phase 2: All Remaining Businesses

Commencing January 1, 2004, *PIPEDA*'s net will cast over all remaining business organizations throughout Canada, unless the appropriate provincial government has proclaimed substantially similar privacy legislation. (s.30 of the *Act*) To date, no substantially similar legislation has been enacted within Ontario, or is imminently foreseeable.

Regardless, if substantially similar provincial legislation becomes enacted in Ontario, federal works will continue to operate under the auspices of *PIPEDA*. One major exception however in the legislation's application will occur starting January 1, 2004. Although federally and provincially regulated corporations, in Ontario, will be governed by *PIPEDA* when they commercially collect and retain personal information, the *Act* demands only that federally regulated corporations adhere to *PIPEDA* in their employer-employee relationship.

Very few parties are exempt from the operation of this *Act*, the largest group being government agencies already controlled by their own privacy legislation. *see* s.4(2).

Beyond the scope of the *Act* are:

- a) federal government organizations already covered by the *Privacy Act*;
- b) provincial or territorial government, and their agents, and;
- c) any organization that collects, uses or discloses personal information solely for journalistic, artistic or literary purposes. s.4(2)(c)

The *Act* is retroactive in effect, meaning, that personal information already collected and utilized by business organizations, is subject to the *Act*'s provisions.

Major Tenents of PIPEDA

Information Officer

Section 4.1 of Schedule 1 of the *Act* demands that every organization appoint an individual(s) who is accountable for the organization's compliance with the *Act*. This position is commonly referred to as the information officer, tasked with the responsibility of overseeing the organizations continuing compliance with the *Act*. The information officer's identity should be provided on request, and normal practice will likely see this person as the main contact within the organization's public posted privacy statement.

Consent

If an organization comes within the *Act* and wants to collect, use, or disclose someone's personal information then, with very few exceptions, informed consent must be obtained. Consent may be deemed to be implied when personal information is surrendered in the normal course of services provided to the customer.

To be safe a company should always get written consent with respect to the collection, use or disclosure of sensitive information. (Schedule 1,4.3.6)

Once collected, the organization can only use or disclose the personal information for the purpose for which the person gave consent when the organization collected it. Even with this consent, the organization has to limit its collection, use, and disclosure of personal information to purposes that a reasonable person would consider appropriate in the circumstances.(s.5(3)) Should an organization desire to use the personal information which exceeds the customer's or employee's original consent, consent must be re-obtained.

The purpose of collecting personal information when obtained by a client or employee, should be clearly explained by the organization. Practical solutions may be the standard use of a small brochure or information sheet outlining what the personal information will be used, accompanied with a signature.

An individual may withdraw their consent at any time. (Schedule 1, 4.3.8)

Security

Personal information that is collected must have appropriate safeguards. This normally means combinations of physical, electronic and organizational controls. Only mixtures of locked cabinets, data passwords, and personnel restrictions would meet the provisions of the *Act*. Schedule 1, s.4.7.3 strongly encourages an appropriate blend of these safeguards, increasing with the sensitivity of the information.

Disclosure and Privacy Statement

Individuals, including employees, have the right to see the personal information that an organization holds about them, and to correct any inaccuracies. (Schedule 1, 4.9)

Organizations must have an orderly system of processing such requests, and must be fully co-operative towards such requests. If the individual contends that any of his or her personal information is wrong, he or she can ask that it be corrected. s.8(3) of the *Act* demands that requests must be responded to within 30 days.

Organizations must also have a privacy policy or statement (Schedule 1, 4.1.4), summarizing the firm's collection, retention and disclosure policies. This privacy policy must be intelligible to the layperson, and publicly accessible. Posting a privacy statement on a firm's website or in a lobby area would likely meet this requirement.

Organizations must also have an internal complaints system. (Schedule 1, 4.10.2) It is envisioned that this system is utilized after the privacy statement has been consulted, the customer has requested their personal information be disclosed, and now believes that a possible violation of *PIPEDA* exists. At least, the organization must have a simple and streamlined complaint procedure that allows for the acknowledgment, investigation, reporting of the complaint, and if necessary corrections.

Destruction

The *Act* (Schedule 1, ss. 4.5 & 4.5.3) demands an organization should destroy, erase or make anonymous personal information about an employee or customer that it no longer needs. Personal information should be disposed of that does not have a specific purpose or that no longer fulfils its intended purpose. The disposal should be conducted in a way that prevents improper access.

Compliance & Consequences

As with any legal framework, business practices should be constructed to ensure continuing compliance. *PIPEDA*'s implementation is governed by the Canada's Privacy Commissioner, an independent Officer of Parliament, with no departmental relationship to such offices as the CCRA or HRDC. The Privacy Commissioner's office has publicly stated that they are most interested in seeking voluntary cooperation and compliance with *PIPEDA*.

That said, *PIPEDA* does grant a variety of enforcement mechanisms once a complaint is lodged with that office. Individuals may file complaints, for contraventions of the *Act* under s.11(1).

Under s.12 of the *Act*, the Privacy Commissioner has full investigative powers, and can order the production of documents, enter premises, compel testimony and receive evidence. The Privacy Commissioner may, with reasonable grounds, also audit the personal information management practices of an organization, under s.18(1) of the *Act*. This power can also be delegated.

If a complaint is determined to be 'well founded', the Privacy Commissioner may make corrective suggestions. Also, s.12(2) of the *Act* specifically demands that the Privacy Commissioner first resolve complaints by means of dispute resolutions such as mediation and conciliation.

The Privacy Commissioner, however, does not have order making powers. Should the corrective suggestions be ignored or the breach continues, the Privacy Commissioner may publicly post the organization's breach in a public fashion. The Privacy Commissioner envisions that publicly posting an organization's failure to maintain the privacy of personal information would have a negative impact on their commercial activities. In addition either the Privacy Commissioner or the complainant may request a remedy from the Federal Court of Canada. (s.14 of the *Act*)

Should a remedy be sought from the Federal Court of Canada, the following orders, in addition to any other remedies it may give, include:

1. an order for the organization to comply with the *Act*
2. an order for the organization to publicly post any corrective action demanded by the Court, and;
3. an award of damages, to the complainant, for any humiliation suffered .

The *Act* also states that it is also an offence to:

- a) destroy personal information that an individual has requested;
- b) retaliate against an employee who has complained to the Privacy Commissioner, and;
- c) the obstruction of a complaint investigation or an audit by the Privacy Commissioner.

If committed, a person is liable to a fine of up to \$10,000.00 on summary conviction or up to \$100,000.00 for an indictable offence. (s.28 of the *Act*)

The Privacy Commissioner's office has proactively campaigned on a spirit of cooperation, largely through education and explanatory guides and services. The Privacy Commissioner's official web site, www.privcom.gc.ca, is a resourceful service, with many useful documents available.

To date, no known action is currently before the courts under the auspices of *PIPEDA*. The comparable compliance provisions of government privacy legislation have largely been, to date, overlooked in favour of negotiated arrangements and accommodations.

At Smith Valeriotte Law Firm LLP we have the expertise and experience to assist you in dealing with *PIPEDA* issues. We can work with you to develop a Privacy Statement, setup the duties of an Information Officer, develop a Disclosure and Complaint procedure, and outline a proper Destruction Processes. Thank you for meeting with us to discuss these issues.