CANADA ENACTS NEW PRIVACY LAW IMPACTING ALL COMPANIES THAT COLLECT PERSONAL INFORMATION FROM INDIVIDUALS

A recent Canadian privacy law will have a broad impact on organizations operating in Canada that collect personal information from individuals for commercial purposes. The Personal Information Protection and Electronic Documents Act ("Act") sets out strict privacy guidelines covering the access, collection, use, and disclosure of personal information. Contravention of the Act's principles could result in fines (of up to $100,000 per offense) or other court-ordered remedies, including damages to the complainant for humiliation suffered. There is no ceiling on court-ordered monetary damages.

Part 1 of the Act, which specifically addresses the protection of personal information in the private sector, is summarized below.

I. PURPOSE AND SCOPE OF THE ACT

The stated purpose of the Act, in part, is to

> establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a *reasonable person* would consider appropriate in the circumstances.[1]

Part 1 establishes rules (for the private sector[2]) governing the access, collection, use, and disclosure of personal information in the course of "commercial activity." Personal information is defined as "information about an identifiable individual," but not including the "name, title or business address or telephone number of an employee of an

---

1 Personal Information Protection and Electronic Documents Act ("Act"), S.C., ch. 5, pt. 1, cl. 3 (2000) (Can.) (formerly Bill C-6) (emphasis added).

2 Canada's federal Privacy Act deals with personal information in the public sector.

organization."[3] "Commercial activity" is defined as "any particular transaction, act or conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."[4] In addition, the Act covers the collection, use, or disclosure of personal information about employees of an organization in connection with the operation of a "federal work, undertaking or business."[5] Although electronic documents are a focus of the Act, the provisions apply to personal information in any form.

The entirety of Part 1 of the Act does not apply to the collection, use, or disclosure of personal information (1) by any government institution to which the federal Privacy Act applies; (2) by an individual where it is exclusively for personal or domestic purposes;[6] or (3) by any organization that uses personal information solely for journalistic, artistic, or literary purposes.

II. SUMMARY OF PART 1 OF THE ACT

The basic requirement of Part 1 is that the consent of the individual must be obtained before personal information is collected, used, or disclosed. Throughout the Act, a "reasonable person" standard is used. The expectations of the individual "determine whether consent must be express, or may be inferred, based on the circumstances."[7]

The individual has both a right to access personal information held by an organization and a right to challenge its accuracy. Use of personal information is limited to the purposes for which it was collected. If an organization is going to use it for another purpose, consent must be obtained again from the individual. Individuals must also be assured that their information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords, or encryption.

---

3 Act, pt. 1, cl. 2(1) (emphasis added). The Task Force on Electronic Commerce lists the following examples of personal information: race, ethnic origin, color, age, marital status, religion, education, medical, criminal, employment or financial history, address and telephone number, numerical identifiers such as Social Insurance Number, fingerprints, blood type, tissue or biological sample, and views or personal opinions. *See* Task Force on Electronic Commerce, The Personal Information and Electronic Documents Act: A Primer on its Privacy Provisions ("E-Com Primer") is *available at* http://e-com.ic.gc.ca.

4 Act, pt. 1, cl. 2(1). The Electronic Commerce Task Force's examples of "commercial activity" under the Act include sales, purchases, barters, and exchanges. *See* E-Com Primer.

5 "Federal work, undertaking or business" is defined in the Act as "within the legislative authority of Parliament." Act, pt. 1, cl. 2(1).

6 The Task Force on Electronic Commerce lists Christmas card lists as an example of this category. *See* E-Com Primer.

7 As an example, the Act explains that an individual subscribing to a magazine could reasonably expect that the organization would contact the person in the future to solicit a renewal of that subscription. Therefore, subscribing to the magazine serves as a means of consent for this specific purpose. However, an individual would not reasonably expect that personal information given to a health care professional would be given to a company selling health care products, unless consent were obtained. *See* Act, sched. 1, cl. 4.3.5.

The following ten substantive principles comprise the bulk of the privacy provisions of the Act.

1. Accountability

The organization shall:

- be responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing,
- use contractual or other means of protection while information is being processed by third parties, and
- designate an individual to be accountable for compliance.

2. Identifying purposes

The organization shall:

- identify the purposes for collection at or before the time the information is collected,
- identify new purposes if they have not been previously identified, and
- ensure that personnel collecting information can explain the purposes for collection.

3. Consent

- Knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except "where inappropriate."
- Organizations shall make a "reasonable effort" to ensure that the individual is advised of the purposes for which the information will be used.[8]
- Consent shall not be obtained through deception.

Exceptions

Knowledge and consent are not required under certain circumstances.

Collection is permitted without knowledge or consent when:

- the collection was clearly in the interests of the individual and consent could not be obtained in a timely fashion,

[8] An organization should seek express consent when the information is likely to be considered sensitive. Implied consent is generally appropriate when the information is less sensitive. *See* Act, sched. 1, cl. 4.3.6. The Act lists medical and income records as sensitive "almost always." Also, the Act explains that sensitivity can be based on context; for example, subscription lists to certain special-interest magazines could be considered "sensitive." *See* Act, sched. 1, cl. 4.3.4.

- it was reasonable to expect that collection with knowledge or consent would compromise the availability or accuracy of information and collection was reasonable for purposes related to investigating a breach of an agreement or a contravention of law,
- information was collected solely for journalistic, artistic, or literary purposes, or
- the information was publicly available.

Use is permitted without knowledge and consent when the information is:

- used or collected for law enforcement,
- used in life-threatening emergencies,
- used for statistical purposes, scholarly study, or research in a manner that will ensure confidentiality, and it is impracticable to obtain consent before the information is used, or
- collected under a consent exception listed above.

Disclosure is permitted without knowledge and consent when the information is:

- disclosed to the organization's legal counsel,
- for debt collection,
- disclosed to comply with a subpoena or warrant,
- disclosed pursuant to a government request (for national security or law enforcement),
- disclosed in a life-threatening emergency,
- to be used for statistical purposes,
- for conservation of historic records,
- a publicly available record, or
- required by law.

4. Limiting collection

An organization shall:

- limit collection to only what is necessary to fulfill the identified purposes, and
- collect information by fair and lawful means.

5. Limiting use, disclosure, and retention

An organization shall:

- not use or disclose personal information for purposes other than those for which it was collected, except with consent, or as required by law (thus the

use, collection, or disclosure of personal information without the individual's consent is prohibited), and
- retain personal information only as long as necessary for the fulfillment of the identified purpose.[9]

Exceptions

An organization may use personal information for purposes other than those for which it was collected when such information is:

- used or collected for law enforcement,
- used in life-threatening emergencies,
- used for statistical purposes, scholarly study, or research in a manner that will ensure confidentiality, and it is impracticable to obtain consent before the information is used, or
- collected under a consent exception listed above.

An organization may disclose personal information for purposes other than those for which it was collected when the information disclosed is:[10]

- disclosed to the organization's legal counsel,
- for debt collection,
- disclosed to comply with a subpoena or warrant,
- disclosed pursuant to a government request (in a national security or law enforcement context),
- disclosed in a life-threatening emergency,
- to be used for statistical purposes,
- for conservation of historic records,
- a publicly available record, or
- required by law.

6. Accuracy

An organization shall:

- keep personal information as "accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used."[11]

---

9 Personal information that is no longer needed for the identified purpose should be "destroyed, erased, or made anonymous." *See* Act, sched. 1, cl. 4.5.3.

10 *See* Act, pt. 1, cl. 7(5).

11 *See* Act, sched. 1, cl. 4.6.

7. Safeguards

An organization shall:

- implement security safeguards appropriate to the level of sensitivity necessary to protect personal information.[12]

8. Openness

An organization shall:

- make "readily available" its personal information management policies,[13] and
- make this information generally understandable.

9. Individual access

An organization shall:

- upon written request, inform individuals of the "existence, use, and disclosure" of their information and provide access to it,
- be as specific as possible when giving an account of the third parties to which their information has been disclosed,
- respond to requests for access in a timely fashion at little or no cost to the individuals requesting access, and
- amend incorrect information and transmit corrections, if justified, to third parties who received incorrect information.

Exceptions

Access need not be granted if:

- the information is protected by the attorney-client privilege,
- access would reveal confidential commercial information,[14]
- access would threaten the life or security of another individual,
- the information was collected for law-enforcement purposes, or
- the information was generated in a formal dispute resolution.

---

12 Safeguards may include file cabinet locks, employee security clearances, and technological measures such as encryption and passwords. *See* Act, sched. 1, cl. 4.7.3.

13 Material made available shall include how to contact the accountable person, how to gain access to personal information held by the organization, how personal information will be used, organization policy regarding personal information, and whether information is made available to other organizations. *See* Act, sched. 1, cl. 4.8.2.

14 If information is severable, the organization must provide access after severing the requested information from other confidential information. *See* Act, pt. 1, cl. 9(1).

10. Challenging compliance

An organization shall:

- implement complaint procedures that are easily accessible and simple to use,
- inform complainants of the appropriate complaint procedures, and
- investigate all complaints, and, if necessary, take appropriate measures.[15]

III. EFFECTIVE DATES

The Act will be phased in gradually. Part 1 became effective on January 1, 2001, and currently applies to the federally regulated private sector, including telecommunications, banking, and interprovincial transportation. Other organizations that transact using personal information interprovincially in Canada or internationally are also required to comply immediately. After one year (January 1, 2002), organizations that collect, use, or disclose personal health information must come into compliance. Finally, after three years (January 1, 2004), the Act will apply to all personal information collected, used, or disclosed in the course of all commercial activity.

The Canadian provinces have three years to pass privacy legislation similar to the federal Act. Those provinces that enact such legislation will be exempt from the federal legislation for intraprovincial flows of personal information. The federal Act will apply within those provinces that do not enact such legislation. Therefore, foreign firms need to be aware of the privacy legislation of the particular provinces in which they conduct business.

IV. REMEDIES

The Act expands the responsibilities of the Privacy Commissioner by empowering him to receive complaints regarding contravention of the ten principles listed above, to conduct investigations, and to attempt to resolve the complaints. The Commissioner may also initiate complaints, if there are reasonable grounds to investigate. If the complaints cannot be resolved by the Commissioner, matters can be taken to the Federal Court for resolution. Court remedies could include (1) ordering an organization to correct its practices to come into compliance with Clauses 5-10 (which provide the privacy requirements); (2) ordering an organization to publish a notice of any action taken or proposed for correcting its practices and (3) awarding damages to the complainant, including damages for humiliation suffered (there are no statutory limits on such damages awards).

Fines may be assessed for up to $10,000 for a summary conviction offense, and $100,000 for an indictable offense. Fines would apply to a person who knowingly (1) contravened the requirement to retain information under clause 8(8); (2) took action,

[15] Appropriate measures may include amending organization policies and practices. *See* Act, sched. 1, cl. 4.10.4.

contrary to clause 27.1, against a whistle-blowing employee; or (3) obstructed the Commissioner or the Commissioner's delegate in the investigation of a complaint or in conducting an audit.

V. CONCLUSION

Various countries around the world are increasingly adopting stringent laws to protect the personal privacy of their citizens, and are backing up these laws with stiff penalties for violations. The new Canadian Personal Information Protection and Electronic Documents Act is one such law that would impact every United States company doing business in Canada. In order to avoid potentially significant liability, all companies that collect, use, or disclose personal information for commercial purposes in Canada, whether online or in paper/manual form, should review their current information practices and privacy policy and make any changes that may be required to ensure compliance with the Canadian law.

If you have any questions about the Canadian law, please call Francis Buono, Pamela Strauss, or Stephanie Podey in our Washington, DC office at (202) 328-8000.

Willkie Farr & Gallagher is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111.

April 27, 2001