FRASER MILNER CASGRAIN

Canada's New Privacy Regime: The Personal Information Protection and Electronic Documents Act

Michael G. Beairsto, Partner

January 19, 2001

Rationale for the Legislation:

- to make Canada's standards for the protection of Personal Information consistent with international data protection standards.
- particular concerns over the ability of European data commissioners to block information transfers with European countries if Canada fails to meet international standards.

Goal of the Legislation:

- to balance the privacy rights of individuals and the reasonable needs of organizations to use an individual's Personal Information.

Federal Legislation:

The Act is made up of Five Parts:

- Part I: deals with the collection use and disclosure of Personal Information (this will be the focus of the presentation)
- Parts 2 to 5: deal with the use of electronic signatures and electronic documents in federal courts and the electronic means of publishing and revising federal legislation.

What does it cover?

"Personal Information" about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

What does it cover?

This presumably includes information such as:

- age, name, ID, income, ethnic origin and blood type
- opinions, evaluations, comments, marital status or disciplinary actions
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services or change jobs)

Application of Act:

Part I applies to every organization in respect of Personal Information that an organization collects, uses or discloses in the course of commercial activities; or is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

Application of Act:

"Commercial activity" means 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.

Three Stages of Implementation:

Stage 1: January 1, 2001 - Federal

The Act applies to private sector federal works and undertakings, including telecommunications and broadcasting companies, banks and airlines, and businesses or organizations that collect, use or disclose Personal Information (except personal health information) across provincial or international borders in the course of commercial activities such as credit reporting agencies or organizations that sell, lease or exchange mailing lists or other Personal Information.

Three Stages of Implementation:

Stage 2: January 1, 2002 - Health Information

The Act extends to personal health information for organizations and activities covered in Stage 1.

"Personal health information" with respect to an individual, whether living or deceased, means:

(a) information concerning the physical or mental health of the individual;

Three Stages of Implementation:

Stage 2: January 1, 2002 - Health Information

(b) information concerning any health service provided to the individual;

(c) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;

Three Stages of Implementation:

Stage 2: January 1, 2002 - Health Information

(d) information that is collected in the course of providing health services to the individual; or

(e) information that is collected incidentally to the provision of health services to the individual (Section 2(1) of the Act).

Three Stages of Implementation:

Stage 3: January 1, 2004 - Everybody

The Act will apply to all private sector entities that collect, use or disclose Personal Information in the course of commercial activities.

Exception: If a province has enacted legislation similar to the Act that effectively regulates commercial use of Personal Information by organizations in that province, the provincial legislation will apply and not the Act.

Three Stages of Implementation:

Stage 3: January 1, 2004 - Everybody

Provinces that have enacted legislation protecting the use of Personal Information in commercial activities: Quebec

Other provinces and territories are considering private sector legislation.

Provinces that have legislation protecting the use of personal health information: Manitoba, Alberta (not yet in force) and Saskatchewan (not yet in force).

Employer-Employee Relationships:

A federally regulated employer will be required to obtain an employee's consent to collect, use or disclose any Personal Information other than name, title, business address or telephone number.

Examples include an employee's earnings, home telephone number, Social Insurance Number, performance evaluations, discipline records and attendance records.

Scenario of the Effect of the Act:

Personal Information provided by Canadian users and collected by a U.S. company on its web site likely falls within the ambit of the Act. It is likely that the Privacy Commissioner would determine that Canada is the situs of the Personal Information collection activity as it is being provided to the U.S. company by Canadian users and therefore, the Act will apply.

Scenario of the Effect of the Act:

Whether the collection of Personal Information is in the course of a commercial activity may depend however on the purpose of the web site. Whether the site has advertising on its pages or provides links to sites that sell products to users, *inter alia*, may be determinative.

Ten Privacy Principles:

The Act incorporates ten principles outlined in the Canadian Standards Association's *Model Code for the Protection of Personal Information*. These principles set out the obligations of organizations when dealing with individual's Personal Information.

Ten Privacy Principles:

1. **Accountability**

   Organizations are responsible for the Personal Information under their control.

2. **Identifying Purpose**

   Organizations must advise individuals why they are collecting the Personal Information and how it will be used.

Ten Privacy Principles:

3. **Consent**

   Organizations are required to obtain an individual's consent to collect, use or disclose Personal Information.

   Exceptions: legal, medical or security reason which makes it impractical to seek consent.

   Consent may be implied or expressly granted.

Ten Privacy Principles:

4. **Limiting Collection**

   Organizations are only entitled to collect minimum Personal Information necessary to fulfil stated goals.

5. **Limiting Use, Disclosure and Retention**

   New uses and disclosure require new consent and the information collected should be kept only for as long as necessary.

Ten Privacy Principles:

6. **Accuracy**

   The information must be kept accurate and as current as necessary to fulfil the stated purpose.

7. **Safeguards**

   Organizations must safeguard individuals' Personal Information to protect against loss, theft, unauthorized disclosure, copying, use or alteration.

Ten Privacy Principles:

8. **Openness**

   Organizations must inform individuals about the Personal Information they hold, the purposes for which it is used, the persons to whom it is disclosed and how an individual may access it.

Ten Privacy Principles:

9. **Individual Access**

   Individuals are entitled to have access to their Personal Information retained by organizations.

   Exceptions: solicitor-client privilege; confidential commercial transactions.

.

Ten Privacy Principles:

10. **Challenging Compliance**
    Internal complaint procedures within the organization collecting and making use of the Personal Information;

    Complaints to Privacy Commissioner; and

    Application to Federal Court by Privacy Commissioner or complainant or for the hearing of a matter before the Privacy Commissioner.

Offences and Penalties:

- Fines of up to $10,000 or $100,000 depending on the nature of the offence.
- Offences include destroying Personal Information of an individual who requested access before he or she has the opportunity to view it, and reprisals against individuals who notify the Privacy Commissioner of violations of the Act.

.

Suggestions for Compliance with the Act:

- Appoint a staff member as the privacy compliance officer for the organization.
- Draft a comprehensive privacy policy outlining, *inter alia*, the purpose for which your organization collects Personal Information, the retention period of the Personal Information and the method by which the individuals may access their Personal Information held by the organization.

Suggestions for Compliance with the Act:

- Obtain consent of customers and other individuals from whom your organization collects Personal Information.
- Establish an internal complaints procedure to resolve individuals' complaints about the use of or access to their Personal Information.

Suggestions for Compliance with the Act:

- Conduct an inventory of the types of Personal Information currently on file and routinely collected or used.
- Establish a method for user's to extend their consent to allow the organization to make use of their Personal Information for a purpose other than the originally stated purpose.

FRASER MILNER CASGRAIN

Business. Advice. Success.

THANK YOU