

## **The *Personal Information Protection and Electronic Documents Act*: What it means for federally regulated businesses and their employees**

On January 1, 2001, Bill C-6, the *Personal Information Protection and Electronic Documents Act* came into force. Part I of the Act deals with the protection of personal information in the private sector, and will have its greatest impact from the perspective of employer-employee relations.

The purpose of Part I is to establish "rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals ... and the need of organizations to collect, use or disclose personal information" for appropriate purposes.

### **APPLICATION**

The Act applies to federally-regulated enterprises, such as banks, telecommunications and transportation companies, and covers the personal information of their employees that is collected, used or disclosed in the course of commercial activities. It does not apply to the personal information of other private sector employees.

Personal information is defined as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization". This exception has been referred to as "business card" type of information about an employee. As of January 1, 2002, the Act will apply to personal health information as well.

### **FUNDAMENTAL OBLIGATIONS**

#### *The 10 Principles of Fair Information Practice*

Every organization must comply with the obligations set out in Schedule 1 of the Act. Schedule 1 contains ten privacy principles developed by the Canadian Standards Association to balance individual privacy rights with legitimate business interests. The following is a brief summary of the principles and what they require:

Accountability:

- Organizations must designate individuals accountable for maintaining compliance.

Identifying purposes:

- Reasonable purposes must be identified before information is collected.

Consent:

- Knowledge and consent of the individual is required before collection, use or disclosure of information, subject to exceptions.

Limiting collection:

- Collection of personal information should be limited to that which is necessary for the purposes identified by the organization.

Limiting use, disclosure, and retention:

- Information collected for one purpose should not be used or disclosed for another purpose without the consent of the individual involved, or as required by law. It should not be retained any longer than necessary for the last specified purpose.

Accuracy:

- Information must be as accurate as necessary for the purposes for which it is used. Decisions should not be made based on inaccurate information.

Safeguards:

- Personal information must be protected in a manner appropriate to its sensitivity.

Openness:

- Companies must communicate their privacy policies and practices.

Individual access:

- Individuals have the right to know what information companies have about them and how it has been used or disclosed. They have the right to have access to the information and to have it amended as appropriate.

Challenging compliance:

- Individuals have the right to challenge a company's compliance by addressing complaints to designated persons in the company or to the federal Privacy Commissioner.

*Appropriate purpose*

Subsection 5(3) of the Act underscores the importance of having an appropriate purpose for the collection, use or disclosure of personal information. There appears to be no exception to the requirement that the purpose be that which "a reasonable person would consider

appropriate in the circumstances".

### *Consent*

Consent is also an important element in the new Act. However, unlike the appropriate purpose rule, the consent requirement is subject to exceptions. The following are some of the exceptions provided in the Act:

with respect to *use* and *collection*:

- if it is clearly in the individual's interests and timely consent is not available;
- if knowledge and consent would compromise the availability or accuracy of the information and collection is required to investigate a breach of an agreement or contravention of the law;

with respect to *use*:

- if the organization has reasonable grounds to believe the information could be useful when investigating a contravention of the law;
- in specified emergency situations;

with respect to *disclosure*:

- to a lawyer representing the organization;
- to collect a debt the individual owes to the organization;
- to comply with court or tribunal order;
- for specified law enforcement purposes;
- in specified emergency situations;
- if required by law.

### *Access*

Within 30 days, the organization must respond with due diligence to written requests for access to personal information or, in specified circumstances, must notify the individual that it requires an extension of up to another 30 days to respond. Failure to respond within the time limit is deemed to be a refusal.

As with consent, there are exceptions to the access principle. For example, an organization *must* refuse access if it would reveal information about a third party, unless there is consent or a life-threatening situation. Circumstances in which an organization *may* refuse access include those where information is subject to solicitor-client privilege or was generated in the course of a formal dispute resolution process.

## **ENFORCEMENT**

### *Complaints*

Individuals may file a complaint with the federal Privacy Commissioner for a contravention of the provisions in respect of personal information protection, or for a failure to follow a recommendation contained in the ten principles noted above. The Commissioner may also

initiate a complaint.

The Commissioner is given wide powers in connection with his or her investigations of complaints, but has no power to make orders. The Commissioner can hold hearings in a manner similar to the courts, enter premises to obtain records, and attempt to settle disputes through mediation or conciliation.

Where, following an investigation, the Commissioner chooses to prepare a report of the investigation, the complainant may apply to the Federal Court in respect of any matter raised in the complaint or the Commissioner's report, provided the matter relates to specified provisions of the ten principles in Schedule 1. Among the Court's remedial powers is the power to award damages to the complainant, including damages for humiliation suffered.

#### *Audits*

The Commissioner may also, on reasonable notice and with reasonable grounds, audit the personal information management practices of an organization. The Commissioner has the same powers in conducting audits as those for investigating complaints. Following the audit, the Commissioner provides the organization with a report containing any recommendations he or she considers appropriate. Significantly, the report may be included in the annual report the Commissioner is required to submit to Parliament.

### **IMPLICATIONS**

It is clear from a review of the Act that, at the very least, new obligations are being placed on employers in the federally-regulated private sector, and new rights are being given to their employees.

#### *Employer Obligations*

Under the accountability and openness principles, employers must designate and train employees to implement and maintain the new privacy protection and access procedures. Under the purposes principle, they must avoid collecting, using or disclosing personal information before an objectively appropriate purpose has been identified. Companies must be mindful of their obligations to respond to access requests within the specified time frames and to not hinder the investigations or audits of the Privacy Commissioner.

#### *Employee Rights*

Employees under federal jurisdiction are now in a position to question whether the employer is collecting, using or disclosing their personal information with their knowledge and consent. With limited exceptions, they have the right to access their personal information and to insist that it be amended or corrected if found to be deficient. They can insist that appropriate safeguards be implemented for their personal information in the employer's possession, and that the employer have collected, used or disclosed the information for an appropriate purpose. All this will have an impact on employer activities such as monitoring programs, and the provision and receipt of employee reference checks.

Moreover, employees now have the right to file complaints with the Privacy Commissioner and to have the matter investigated. In many cases, the Commissioner's investigation will result in a report being prepared, which in turn may allow the employee to apply to the

Federal Court for relief.

#### *Whistleblower protection*

Employers are prohibited from retaliating against an employee who, in good faith and with a reasonable belief, reports a violation, refuses to commit a violation, or acts to prevent a violation.

#### **In Our View**

Although the Act applies only to workplaces in the federally-regulated private sector, similar legislation is clearly in the offing for businesses under provincial jurisdiction in Ontario. Employers should therefore start thinking now about how such legislation will affect their operations, and the policies that will need to be implemented to maintain compliance. This will be the subject of an article in the next issue of *FOCUS* (see "[Ensuring compliance with the Personal Information Protection and Electronic Documents Act: what your organization should do](#)". For more information on privacy legislation, please see "[Ontario releases draft privacy legislation](#)".)

For further information, please contact [Colleen Dunlop](#) at (613) 563-7660, Extension 222 or [Steven P. Williams](#) at (613) 563-7660, Extension 242.

For more news about recent developments in Employment and Labour Law, and for information about how our firm can assist you, please visit <http://www.emondharnden.com/>