EMOND HARNDEN
LABOUR & EMPLOYMENT LAW
DROIT DU TRAVAIL ET DE L'EMPLOI

Ontario releases draft privacy legislation

April 1, 2002

The Ontario government has released a consultation draft of the proposed *Privacy of Personal Information Act, 2002* (*PPIA*). If passed by the Legislative Assembly before January 2004, the legislation will pre-empt the application of the federal privacy statute to provincially regulated businesses in Ontario (see "The *Personal Information Protection and Electronic Documents Act*: What it means to federally regulated businesses and their employees" on our Publications page).

The *PPIA*, like its federal counterpart, is intended to reflect the ten privacy principles developed by the Canadian Standards Association. However, it differs from the federal Act in that it has extensive specific provisions governing "health information custodians" — defined to include a broad range of persons and organizations in the health sector — and the privacy of personal health information, whether held by health information custodians or organizations outside the health sector. This article will deal principally with the non-health-related aspects of the legislation.

APPLICATION

While the federal Act applies to federally regulated entities, such as banks and telecommunications companies, that are engaged in commercial activities, the proposed Ontario law would apply to "organizations", which are broadly defined to include persons, incorporated or unincorporated associations, trade unions and individuals, except where the individuals are acting in a "personal and non-commercial capacity". Provincial public sector organizations will continue to be governed by the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and *the Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*).

INDIVIDUALS' RIGHTS

As with the federal legislation, the *PPIA* attempts to balance individuals' privacy rights with the need of organizations to collect, use or disclose personal information for reasonable purposes. The principal privacy entitlements conferred on individuals by the Act are as follows:

a) To provide or withhold consent to the collection, use and disclosure of one's personal information.

Consent may be express or implied. However, consent to the collection of personal health information by a non-health sector organization must be express. Consent to collection, use or disclosure of personal information may be implied only if:

- the purpose of the collection, use or disclosure is reasonably obvious to the individual;
- it is reasonable to expect that the individual would consent; and

- the organization uses or discloses the information only for the purpose for which it was collected.

b) To be informed of one's rights with respect to the collection, use and disclosure of one's personal information.

c) To have access to one's personal information and the ability to challenge both its accuracy and completeness.

The right to access is made subject to a number of exceptions related to security, law enforcement, privilege, third-party privacy and trade secret considerations. If the personal information has previously been released to a government or investigative body, that government or body has the right to object to its release. Other individuals whose personal information would be revealed if the information were released may also withhold their consent to its release to the requesting individual.

Requests for access must be in writing, and organizations must generally respond to the request within thirty days. If the individual requesting access asks for assistance in making the request, the organization must provide it. An individual may also request information about the use and disclosure of the personal information and, if access is granted, this information must also be released. An individual whose request has been refused or not dealt with within the time limit may complain to the Information and Privacy Commissioner.

d) To have access to a fair and independent overseeing body to address complaints regarding compliance with the Act.

The oversight function is granted to the Information and Privacy Commissioner, the same person who administers *FIPPA* and *MFIPPA*. Allegations of violations of the Act may come before the Commissioner by way of a complaint, or the Commissioner may initiate his or her own review if satisfied on reasonable grounds that a violation has been or is about to be committed.

The Commissioner may appoint inspectors to investigate alleged violations. These persons have the power to enter premises and demand production of documents and records. After reviewing a complaint, the Commissioner may make orders, including orders directing the organization to:

- cease collecting, using or disclosing personal information in breach of the Act;
- change, cease or not commence an information practice that is in breach of the Act;
- dispose of information;
- implement a practice;
- perform a duty imposed under the Act;
- grant an individual access to personal information; and
- correct personal information.

The Commissioner's order may be appealed to the Divisional Court, but only on questions of law, not fact. Once appeal rights have been exhausted, the Commissioner's order may be filed in court and it then becomes enforceable as a court order. As well, an individual in respect of whom a final order has been made may sue in court for damages for actual harm suffered as a result of an organization's breach of the Act.

ORGANIZATIONS' DUTIES

The Act's purpose of governing the collection, use and disclosure of personal information is to be achieved by way of duties and obligations placed on organizations. For example,

a) Organizations are responsible for personal information in the custody or control of the organization and for designating individuals accountable for the organization's compliance with the *PPIA*.

Organizations must have information practices in place that comply with the Act, and must act in conformity with those practices. They must make public a written statement describing their information practices, and how individuals may contact the designated person responsible for compliance, access their personal information and make a complaint about non-compliance.

b) Organizations must obtain an individual's consent before collecting, using or disclosing personal information.

The Act sets out a number of circumstances where consent to collection need not be obtained, such as:

- when collection is clearly in the interests of the individual and consent cannot be obtained in a timely way, and the organization notifies the individual in writing of the purpose of the collection and that it is collecting information without consent under the authority of the Act;
- in specified law enforcement or investigatory contexts; and
- in emergency circumstances relating to the life, health or security of the individual.

There are also provisions designed to allow personal information to be collected and disclosed without consent so as to permit most sales of businesses by way of asset sales. However, if the personal information constitutes all or almost all of the assets of the business, or if the successor owner of the assets will not be carrying on a substantially similar business, consent must still be obtained.

Further, personal information may be disclosed without consent if an organization discloses the information to another organization or to its professional advisors; the disclosure is necessary for the organization to perform its functions properly; and the organization or advisors receiving the information are bound to maintain its confidentiality and to not use it for any function other than the functions of the disclosing organization.

c) Organizations are also required:

- to take all reasonable steps to ensure the accuracy of records of personal information;
- not to update records of personal information unless the updating is necessary to fulfill the purposes for which the information was collected, and it is consented to by the individual or permitted by law;
- to maintain the security of personal information with safeguards appropriate for its sensitivity, and to protect it from unauthorized use, disclosure, copying, modification or destruction;
- to note instances of use and disclosure of personal information without consent; and
- subject to certain exceptions, not to retain personal information after the purpose for which it was collected has been accomplished, and to destroy or delete the information once that purpose has been accomplished.

There are also broadly stated obligations on employers not to collect, use or disclose personal information if other information will serve the purpose, and not to collect, use or disclose more personal information than is reasonably necessary.

OTHER PROVISIONS

Whistleblower protection

Like the federal legislation, the *PPIA* contains provisions prohibiting organizations from retaliating against persons who, in good faith and based on reasonable belief, report a violation of the legislation, act to prevent a violation or refuse to commit a violation.

Offence provisions

The Act provides for maximum fines of $50,000 and $250,000 for individuals and corporations respectively. Offences include:

- using deception or coercion to collect, use or disclose personal information;
- obtaining access to personal information when a person has reason to believe he or she is not entitled to access;
- disposing of a record of personal information with intent to evade a request for access;
- obstructing the work of the Commissioner;
- knowingly misleading or making a false statement to the Commissioner;
- failing to comply with an order of the Commissioner; and
- retaliating against a whistle-blowing employee.

In Our View

Like the federal Act, the Ontario legislation will, if it becomes law, give employees the right to question how their personal information is being used. Further, the Information and Privacy Commissioner, unlike his or her federal counterpart, will have an order-making power in respect of

employee complaints. This may make the idea of filing a complaint more appealing to individuals whose employers fall under the provincial privacy regime than to those whose employers are regulated under the federal system.

The draft legislation is extremely complex due to the fact that it combines privacy provisions of general application with provisions specific to the health sector and health information. The Information and Privacy Commissioner has already commented on the complexity of the draft's structure. The consultation period ended on March 31, 2002. Readers will be advised of developments as the legislation makes its way towards becoming law.

For further information, please contact Jennifer Birrell at (613) 563-7660, Extension 261.