THE *PERSONAL INFORMATION AND ELECTRONIC DOCUMENTS ACT*: A PRIMER ON ITS PRIVACY PROVISIONS

Part 1 of the Act provides privacy protection for personal information that is collected, used or disclosed in the private sector. Canada already has federal and provincial legislation to protect personal information which is collected and used by governments, with the exception of PEI. Quebec is the only province to date that has enacted privacy legislation which applies to the private sector.

How does it protect personal information?
Personal information is defined as "information about an identifiable individual," and includes things such as race, ethnic origin, colour, age, marital status, religion, education, medical, criminal, employment or financial history, address and telephone number, numerical identifiers such as the Social Insurance Number, fingerprints, blood type, tissue or biological sample, and views or personal opinions. Protection of this information is achieved by requiring organizations to comply with the obligations in CSA International's Model Privacy Code. The Code is brought into the law, and indeed becomes the law, by being incorporated as Schedule 1 to the Act.

Where and when will it apply?
The Act will eventually apply to every organization that collects, uses or discloses personal information in the course of commercial activity. Commercial activity is any activity that is of a commercial character and would include sales and purchases as well as activities such as barters and exchanges. An organization includes a company, an association, a partnership, a person or a trade union. It does not apply when an organization uses personal information solely for journalistic, artistic or literary purposes and it does not apply to personal information used solely for personal or domestic purposes, such as Christmas card lists.

To encourage harmonization of provincial and federal privacy protection laws, the Act adopts a phased-in approach. On January 1, 2001, it will apply to the federally-regulated private sector, including telecommunications, broadcasting, banking and interprovincial transportation, in respect of both customer and employee information. It will also apply to an organization that discloses personal information across provincial or national borders for consideration (e.g., selling, bartering or leasing), such as credit reporting agencies. The Act will apply to organizations that collect, use or disclose personal health information on January 1, 2002, which will give the health sector more time to get their systems and procedures ready. On January 1, 2004, the Act will apply more broadly - to all personal information collected, used or disclosed in the course of all commercial activity. If, however, a province passes a law that is substantially similar to the federal Act, the organizations or activities covered by the provincial law will be exempted from the federal law for collection, use or disclosure within the province. The federal Act will continue to apply to all interprovincial and international collections, uses or disclosures of personal information. Quebec has had a substantially similar law since 1994.

What obligations will an organization have to meet?
Basically, an organization will have to meet the obligations of Schedule 1. Schedule 1 contains 10 principles that are explained and elaborated in sub-clauses, sometimes by way of example. Since it applies to all industry sectors and to companies of all sizes across the country, the principles are general. The Schedule also gives organizations the flexibility to adapt the principles to their particular operations.

The 10 principles, in a nutshell, relate to accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access, and challenging compliance.

Are there any exceptions?
There are a few exceptions to the general requirement to obtain an individual's consent. These exceptions cover such situations where the collection clearly benefits the individual, or obtaining consent would compromise the information's accuracy, where the data is required for a legal investigation or aid in an emergency where lives and safety are at stake, or if a disclosure would facilitate the conservation of historically important records.

What is the most important thing for individuals and organizations to know?
A key principle in Schedule 1 is the requirement for organizations to obtain an individual's consent when they collect, use or disclose the individual's personal information. The general rule is that no one else will be able to make use of a person's personal information without that person's permission. An individual will have a right of access to their personal information that is held by an organization and to have it corrected, if need be. Personal information can only be used for the purposes for which it was collected and if an organization is going to use it for another purpose, consent must be obtained again. Individuals should also be given the assurance that their information will be protected by specific safeguards, like locked cabinets, computer passwords or encryption.

What can an individual do if his or her personal information is misused?
The first thing to do is to try to settle the matter directly with the organization. All organizations are required to designate an official to deal with privacy issues and this is the person to contact. If not satisfied, the individual can complain to the federal Privacy Commissioner.

What will the Privacy Commissioner do?
The Privacy Commissioner will investigate the complaint, using various powers given by the Act. The Commissioner is an ombudsman who will attempt to resolve the dispute through mediation and persuasion. Once the investigation is completed, the Commissioner will issue a report to the parties with the findings and recommendations. The Commissioner can also initiate a complaint or conduct an

audit (with reasonable notice) of the information management practices of an organization and can publish the results, where that would be in the public interest. The Commissioner has a broad mandate to promote the purposes of the Act by conducting public education programs, undertaking research and encouraging organizations to develop privacy policies and practices.

What if the individual is still not happy?

Within 45 days of receiving the Commissioner's report, a complainant can ask for a hearing in Federal Court. The Court has the power to order an organization to correct its practices if they do not comply with the law and to publish notices of any action it has or will take to correct its practices. The Court can also award damages to the complainant, including damages for humiliation.

Won't it be costly to go to Federal Court?

The Act provides that an application to the Federal Court will be heard and determined without delay. The proceeding will be "in a summary way", that is, streamlined and easy. The Commissioner can also take the issue to Court on the complainant's behalf.

Are there offences under the Act?

Anyone who obstructs the Commissioner in an investigation or who destroys records before all recourse is exhausted or who dismisses or disciplines a whistle blower is guilty of an offence and is liable to a maximum fine of $100,000.

Conclusions

The Act provides protection for personal information in a manner that is balanced and fair to both organizations and individuals. It establishes the Privacy Commissioner as an ombudsman, with the goal of obtaining a resolution of privacy disputes in a non-confrontational manner. Through the use of audit, conciliation, education and publication powers, the Commissioner will be able to encourage organizations to comply with the obligations in Schedule 1. For organizations, the principles in Schedule 1 allow for flexibility in meeting the law. Organizations will generally not be subject to fines under the law and they will be given the opportunity to directly solve problems with their clients.