KNOW*law*™

Bulletin

A Report on
New Legal Developments

April 2000

Privacy Law's Bite May Be Worse than its Bark

Something big has come out of Ottawa and one thing is certain: it *will* affect you.

On April 4, 2000, the federal Parliament passed the *Personal Information Protection and Electronic Documents Act*, comprehensive legislation designed to support and promote electronic commerce in Canada. The new law is the culmination of a pledge the government made in 1996 to enact legislation to protect personal information in the private sector by 2000.

Part I of the Act, expected to be proclaimed in January 2001, basically mandates how businesses may use, collect and disclose information about individuals. Part II provides electronic alternatives to meet requirements in existing laws, introduces the concept of *secured signatures*, and explains how Canadian courts will accept and assess electronic documents and signatures. It is anticipated that Part II could be proclaimed as early as May 2000.

The Act's privacy provisions will affect every business in Canada by 2004, with some feeling the effects as early as 2001. Most businesses will need to look hard at how they conduct business, and many will find themselves investing considerable resources in readying their operations for compliance.

This bulletin is the first in a two-part series by McMillan Binch summarizing the new law and exploring its potential impact on Canadian business. In this bulletin, we focus on the Act's privacy component and offer practical tips to companies preparing for its enactment. In the next bulletin, we will turn our attention to standards for electronic documents and related issues.

Why Privacy Legislation and Why Now?

In a very real sense, this law reflects the rapid growth of technology and electronic commerce in Canada and throughout the world. Estimated at about $45 billion in 1998, electronic commerce conducted over the Internet in Canada is expected to exceed $600 billion by 2002. According to the federal government, electronic commerce will not really flourish unless people start to feel confident that their privacy will be protected. Canadians reportedly are apprehensive about the level of protection currently securing their personal information. The new legislation attempts to balance individual privacy concerns against the high value that the modern knowledge-based economy places on the sale and exchange of customer information.

The Act is also a by-product from similar legislation introduced both internationally and in Quebec. In 1984, the OECD developed the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Although Canada formally accepted the guidelines and brought public sector rules into line, the government took no action to implement them through private sector legislation until now. By contrast, Quebec enacted one of the most far-reaching privacy acts in the world in 1994.

Perhaps the single greatest spur to enact legislation today, however, has been the European Union's 1995 release of its Data Protection Directive. The Directive, which took effect October 1998, requires a toughening of the fifteen member states' privacy laws. Each member country must pass legislation limiting the collection of personal information to

Getting Your Business Ready:
Ten Steps You Can Take to Prepare for the New Law

1. Designate a staff member to be responsible for all privacy matters.
2. Establish policies and procedures for protecting privacy and addressing related complaints. Train staff to adhere to privacy policy and procedures, and develop public explanations of your policy and procedures.
3. In your contracts and agreements with outside contractors, ensure the same protection for personal information processed by third parties.
4. Document the purposes for which all personal information is collected.
5. Incorporate a method for obtaining consent to collection, use or disclosure of personal information into application forms, standard contracts or other such documents.
6. Establish procedures for obtaining further consent if information is needed for a purpose other than that originally stated.
7. Develop and implement guidelines for retaining and disposing of personal information.
8. Design safeguards to secure personal information, tailored to the format in which the information is stored.
9. Develop a policy for making personal information available to subsidiaries and other related organizations.
10. Establish procedures to allow individuals access to their personal information, and to correct or up-date information when appropriate.

specified, legitimate purposes; requiring explicit consent to the collection, use and disclosure of personal information; and directing the private sector to institute technological and organizational measures to protect personal information. Each law must also provide for an independent authority to monitor compliance and a judicial remedy for violation.

From Canada's perspective, the Directive's most significant provision is Article 25, which prohibits member countries from transferring personal information to non-member countries whose laws or other security measures do not ensure a comparable level of protection. In practice, this provision could prevent a European branch office from transferring personal customer information to its home office in North America. Similarly, hotels, airlines and credit card companies could be blocked from trading information with and, maybe even doing business in, the EU. The provision has raised major concern outside the EU, particularly in the US. Unlike Canada, the US has taken a firm stance against passing responsive legislation, insisting that contractual measures and business self-regulation afford adequate protection. To date, negotiations between the US and the EU continue. Canada's Act likely meets the EU's standards, since the EU already has reacted favourably to the Canadian Standards Association (CSA) Model Guidelines that form the core of the Act.

How the Privacy Provisions Work

The Act's Coverage

Part I protects all personal information about an identifiable individual. Under the Act's definition, *personal information* includes such data as race, ethnic origin, age, financial history and personal opinions, but does not cover the name, title, business address or telephone number of an organization's employees. Because the definition's original limitation to "information recorded in any form" was deleted from the final version of the Act, the law will likely protect such personal information as blood type, DNA, and blood samples as well.

The law applies to any organization that collects, uses or discloses personal information in the course of commercial activity. Although clearly drafted with companies whose primary business is trading or selling personal information in mind, the Act applies to any private enterprise that deals with personal information. *Commercial activity* is defined broadly to include a range of activities such as sales, purchases, barters, exchanges, and leases of individual personal information or membership and other fundraising lists. Expressly excluded from coverage are hospitals, health clinics and physicians, and any information used exclusively for journalistic, artistic or literary purposes. Information used for purely domestic purposes, such as Christmas card lists, is also exempt.

Timing of the Act

Once proclaimed, the privacy provisions will immediately apply to the federally regulated private sector, including telecommunications, broadcasting, banking and inter-provincial transportation companies. In this initial phase, the privacy provisions will also cover any organization that trades in personal information in more than one province or country.

Within three years of the law's operation, around January 2004, the Act will apply to all private sector companies collecting, using or disclosing personal information in any province, unless the province has passed a law substantially similar to the federal Act. In such circumstances, the Federal Cabinet may grant an exemption from the law's coverage for information dealt with exclusively within the province. Quebec

has had parallel legislation since 1994, and other provinces currently are in the process of drafting or considering similar statutes.

What the Act Means for Your Business

Under the Act's basic scheme, no organization may collect, use or disclose personal information without first clearly defining its purpose and obtaining the individual's consent. Moreover, the organization's purpose must be one that a reasonable person would consider appropriate under the circumstances. The Act also regulates how long information may be held, individual access to the information, and the means to complain about and seek redress for violations.

Through an attached schedule, the Act incorporates the ten principles outlined in the CSA's *Model Code for the Protection of Personal Information*. However, the Act also contains a fairly extensive series of exemptions from and exceptions to the CSA model, which many commentators suggest unduly complicate the law and make it difficult to interpret. What do each of the ten principles require your business to do under the Act?

Accountability

Under the Act, companies must appoint someone within their organization to bear ultimate responsibility for compliance with the privacy provisions, and must identify that individual upon request. Companies must also implement policies and practices to protect personal information and handle complaints from individuals about how the company uses the information. Staff will have to be trained to adopt the policies and practices, and contracts should be structured to ensure the same protection for personal information held by the company but processed by third parties.

Purpose

Before collecting any personal information from an individual, companies must identify and explain their purpose for collecting the information. The purpose may be identified orally or in writing, depending upon how the information will be collected. For example, companies gathering personal information through a written application form probably may explain their purpose directly on the form. In any case, the company's purpose should be documented in writing, and only information necessary to achieve the identified purpose should be collected.

Consent

Another major principle requires companies to obtain the individual's consent to the collection, use or disclosure of personal information. The form and manner of consent required depend on the information's sensitivity and the surrounding circumstances. Thus, in some cases individuals may consent orally over the telephone, or by simply marking a check-off box on an application form. Companies are precluded from obtaining consent through deception, or from making consent a condition to service, except as needed for a legitimate and expressed purpose. Subject to legal or contractual impediments, individuals may withdraw their consent at any time.

The Act deviates significantly from the Model Code's consent provisions by including a number of detailed exemptions. For instance, consent is not required to collect information needed to investigate a breach of contract or violation of the law, where obtaining consent might compromise the information's accuracy. Consent to use is not required where, among other things, the information is used in a criminal investigation, in response to an emergency threatening individual life, health or safety, or in scholarly research or for statistical purposes. Information may be disclosed without consent to the organization's lawyer, or, for instance, to assist in collecting a debt owed to the company or comply with a subpoena, warrant or court order.

Collection, Use, Disclosure and Retention

Under the Act, companies are no longer allowed to indiscriminately amass personal information. Rather, the new law restricts collection to information needed for the company's identified purposes. Once collected, information can be used only for that purpose, unless the individual consents to or the law requires another purpose. Personal information may be held only for as long as necessary to meet the stated purpose. Where information is used to make a decision about someone, however, the company must hold onto the information long enough to allow the person access after the decision is made.

Accuracy and Access

To ensure that decisions about individuals are not based on inappropriate information, companies must keep the personal information they hold as accurate, complete and current as the circumstances require. On the other hand, companies may not routinely update personal information where current information is not needed to achieve the original purpose.

The Act also gives individuals the right to access to their personal information, and to know of the existence, use and disclosure of any information about them. In conjunction with the right to access, individuals may require businesses to amend incorrect information, and transfer those amendments to third parties who also have access to the information. In general, companies must respond to requests for access within thirty days, and any refusal must be in writing accompanied by reasons. However, the Act outlines several situations where access may properly be denied.

Protective Mechanisms

Companies must take affirmative steps to safeguard personal information from loss, theft, unauthorized access, disclosure, use or modification. Depending on the format in which the information is held, this might include physical measures, such as locked cabinets, or technological measures, like encryption and passwords. Information about a company's privacy policy and practices must be readily available, and companies must implement and advise individuals of an internal mechanism for responding to and investigating complaints.

How the Act Is Enforced

Privacy Commissioner's Powers and Duties

Those dissatisfied with a company's response to complaints about how their personal information is managed or to a request for access may file a further complaint with the federal Privacy Commissioner. The Commissioner may also initiate complaints where there are reasonable grounds to launch an investigation. The Act grants the Commissioner broad powers to investigate complaints, including authority to administer oaths, compel individuals to appear, testify and produce evidence, and enter premises other than residences to examine and copy records.

Following investigation, the Commissioner will attempt to resolve the controversy through mediation or conciliation. In most cases, the Commissioner will be required to report on any recommendations within one year of the investigation.

In addition to the power to investigate and mediate complaints, the Commissioner is empowered to audit a company's personal information practices if reasonable grounds suggest that the company has fallen short of the law's requirements. In conducting audits, the Commissioner possesses the same extensive investigatory powers. Audited companies will receive a report of the Commissioner's findings. The findings may also be included in the Commissioner's annual report to Parliament, or published when notice would serve the public interest.

Federal Court Remedies

The Act contemplates the Federal Court's involvement to deal with the Commissioner's actions. The court may order a company to correct its practices and publish notice of its proposed or taken actions, and may award damages, including punitive damages and compensation for humiliation.

Additional Measures

Companies should also be aware of the Act's *whistleblower* provision, which allows the Commissioner to keep the identity of anyone who reports a violation confidential on request. The section also expressly protects employees who report their employers to the Commissioner in good faith, by prohibiting retaliatory dismissal, demotion or other reprisals.

Finally, anyone who obstructs a Commissioner's investigation, destroys records before remedies have been exhausted, or violates the whistleblower provision may be fined up to $100,000.

Conclusion

Despite the Act's staggered implementation scheme, businesses are wise to begin preparing for its application now. Be advised, however, that the new law is complex, and the above represents only a summary of some of its key features. Readers are cautioned against making any decisions based on this material alone. Rather, a qualified lawyer should be consulted.

In the next issue, we will discuss standards for electronic documents and related issues.

For further information, please contact:

John Clifford 416. 865.7134 john.clifford@mcmillanbinch.com

McMillan Binch LLP

Telephone: 416.865.7000
Facsimile: 416.865.7048
Web: www.mcmillanbinch.com

BCE Place, Suite 4400, Bay Wellington Tower, 181 Bay Street, Toronto, Ontario, Canada M5J 2T3