CANADA'S NEW PRIVACY LAW: STRATEGIES FOR COMPLIANCE

Bryan Schwartz

The International Context for Privacy Laws

European Union:

- The 1995 Data Protection Directive requires member states to establish national laws protecting personal information;
- The EU insists that personal information only be sent to non-EU destinations where it will be adequately protected;
- Individual countries may add to minimum EU requirements.

Canada:

- On April 13, 2000, Royal Assent was given to PIPEDA, the Personal Information Protection and Electronic Documents Act;
- PIPEDA was enacted in part to ensure that Canadian destinations are adequate by EU standards;
- As of January 1, 2001, PIPEDA applies to the federally-regulated private sector and to organizations that export data for consideration;
- PIPEDA allows the provinces three years in which to enact "substantially similar" laws to protect privacy;
- As of January 1, 2002, PIPEDA applies to the collection of personal health information.
- As of January 1, 2004, PIPEDA will apply directly in any province to the extent that it has not enacted such laws;
- The Privacy Commissioner can initiate privacy audits of organizations and can make recommendations in response to c o m - plaints by individuals. The Federal Court can issue damage awards and order compliance.

United States:

- There is no comprehensive national-level privacy law governing the private sector;
- Congress has enacted some industry-specific privacy laws;
- US enterprises can obtain designations as privacy "safe havens" in order to receive EU data.

The Province of Manitoba:

- The Freedom of Information and Protection of Privacy Act addresses personal information held by public bodies;
- The Privacy Act protects privacy generally and permits civil actions.
- "The Personal Health Information Act" protects patient privacy.

Essential Elements of a Compliance Strategy

Organizations should aim to meet the requirements of both laws that already apply and of *laws that may apply in the future* – e.g., in the event that data is later moved across a boundary or an organization is sold to, or merges with, a foreign entity.

A COMPLIANCE STRATEGY CAN INCLUDE THE FOLLOWING MEASURES:

Conducting Audits: Audits can be conducted to identify the extent to which business practices meet legal privacy requirements or must be modified. A company that conducts its own internal audit is well positioned to deal with potential audits from the government under the authority of the new privacy statute. Both lawyers and experts in information technology may be needed to conduct a proper audit;

Drafting Formal Privacy Policies: A company should have in place a privacy policy statement. It can both inform and reassure customers and employees. Privacy policy statements can create legally enforceable expectations and should be drafted with the benefit of legal advice;

Drafting Privacy Provisions in Employer, Customer, and Corporate Contracts: Drafting must be sensitive to legal requirements and to the commercial needs of the company. "Reasonableness" is a pervasive requirement of the federal privacy law.

Setting up Information Technology Systems that Maximize Legal Compliance, Security, and Accessibility: Information technology man-

agement consultants and lawyers should work together to ensure that information technology systems comply with both security and accessibility requirements;

Putting in Place the Appropriate Bureaucratic Systems to Monitor Compliance with Legal Requirements and Respond to Requests or Complaints: Businesses must designate officials to respond to requests from individuals. These requests may pertain to information a business has on its files about an individual. They may also be requests to correct misinformation;

Putting in Place Systems to Delete Stale Data: Information cannot be retained for longer periods than is reasonably needed. In order to avoid or alleviate potential problems, stale data must be deleted.

10 Basic Principles of the New Legislation

PIPEDA includes a schedule that sets out ten basic principles that must be observed. They concern the collection, retention, and disclosure of information about an identifiable individual. The latter can be a third party or an employee or officer of an organization. PIPEDA addresses information about an identifiable person; the information need not be particularly sensitive. The fact that a person subscribes to *The Economist* magazine, for example, is "personal information."

THE PRINCIPLES, AS LAID OUT BELOW, OUTLINE WHAT STEPS MUST BE TAKEN BY AN ORGANIZATION.

1. **Accountability:** Organizations must designate staff who are responsible for compliance with the legislation, and put in place the necessary principles and policies to ensure compliance.

2. **Identifying purpose:** Organizations must identify and disclose the purpose for which they are collecting information. If information is gathered for one ostensible purpose, the organization cannot use it for another purpose unless it goes back and obtains consent from the individual who provided the personal information.

3. **Consent:** Organizations must obtain the consent of individuals before collecting, using, or disclosing information about them. Organizations must explain the purposes for which information will be used in a manner that is reasonably understandable.

Sometimes consent can be implicit. If an individual subscribes to an organization's magazine, for example, it can be reasonably inferred that the individual agrees that the organization can use the subscriber list to send out renewal notices. If information is sensitive, the organization should take care to obtain express consent.

4. **Limiting collection:** Organizations can only collect information that is necessary for the purposes it has identified. Organizations cannot collect information indiscriminately. They must obtain information by fair and lawful means. Deception is unacceptable.

5. **Limiting use, disclosure, and information:** Organizations cannot use or disclose information for any purposes other than those for which consent was originally obtained – unless they obtain fresh consent for those new purposes. Organizations cannot keep information for longer than is necessary to achieve their identified purposes. Organizations should have in place guidelines as to how long information can be kept and how it is destroyed.

6. **Accuracy:** Organizations must ensure that information is as accurate and up-to-date as is necessary to achieve the purposes the organization has identified. They must avoid using inappropriate information when making a decision about an individual.

7. **Safeguards:** Organizations must have in place safeguards that are commensurate with the sensitivity of the information. They must protect the information against unauthorized access or use, including theft by third parties. Security measures should include physical protection (such as locked filing cabinets); organizational measures (such as security clearances and limiting access to a "need to know basis"); as well as technological measures (such as the use of passwords or encryption).

8. **Openness:** Organizations must make readily available to individuals specific information about their information policies and practices. The information must be "readily understandable." Organizations should be prepared to identify the staff responsible for compliance, including dealing with inquiries and complaints.

9. **Individual Access:** An individual has the right, upon request, to know what information an organization has about that individual and how the organization is using it.

10. **Challenging Compliance:** Procedures must be in place so that an individual can challenge inaccurate information and have it corrected. The individual should be informed as to who the appropriate staff are for hearing complaints. The procedures should be accessible and simple to use.

15 Potential Pitfalls to Developing a Compliance Strategy

1. **Time Traps:** Some provincially regulated businesses may consider the fact that they will not be subject to PIPEDA, or a provincial equivalent, until as late as January 1, 2004. But when PIPEDA finally does apply, it will not "grandfather" data that has been gathered earlier. A business may find that it possesses much data it can no longer retain. The solution: businesses should bring themselves into compliance with PIPEDA as soon as possible.

2. **Cross-border Traps:** Businesses that are generally regulated by the provinces may overlook this fact: the new federal law applies to them immediately to the extent that they are moving information across a boundary "for consideration." This might easily happen in a routine business transaction or as a result of a merger or acquisition. The solution, again, is for a business to bring itself within the general requirements of the new federal privacy law as quickly as possible.

3. **Organizational Traps:** Different members of a corporate family are different organizations for the purposes of the new federal privacy law. Data held by one member of the family cannot necessarily be transferred to another. Corporate families should develop a harmonious set of privacy practices, including those relating to consent forms and information technology systems, that permit the reasonable sharing of information relating to customers and employees.

4. **Jurisdictional Traps:** A business that focuses exclusively on the privacy laws of its home base may discover that its practices are not compliant with the requirements of other jurisdictions. As a result, the business may not be able to carry out a cross-border merger or acquisition or execute a business transaction that moves personal information across a boundary. The solution: businesses should adopt privacy practices that are compliant with the most demanding requirements of the different jurisdictions with which they might eventually interact. Businesses can also consider having themselves certified as "privacy safe" by an agency whose certifications are widely recognized.

5. **The Illusion-of-Consent Trap:** This pitfall arises when a business thinks that it has overcome privacy laws by asking consumers and employees to sign blanket consent forms for the use of information. Such consents might not be valid under the new federal privacy law. Consumer protection laws in various jurisdictions or common law principles about proper notice and explicitness may similarly invalidate sweeping consent forms. Businesses should be reasonably specific in their consent forms about the legitimate purposes for which they intend to use data.

6. **The Third Party Trap:** A business may be unaware that it might not be able to share certain information with third parties, such as consultants, without complying with legal requirements concerning customer and employee consent. Customer and employee consent forms should provide for third-party access for specified and legitimate purposes. Businesses should also ensure that third parties sign confidentiality agreements.

7. **The Inaccessibility Trap:** Under the new federal privacy law various individuals, including customers and employees, have the right to know what personal information a business is keeping about them. Information about a person must not only be kept safe from unauthorized uses and users, but must also be readily retrievable and available when that person requests it. Privacy policies and practices, including information technology systems, must be designed accordingly.

8. **The Shifting Purposes Trap:** The shifting purposes trap arises when a company that obtains information for one stated purpose is prohibited by law or contract from using it for some other purpose. The solution to this potential pitfall includes drafting consent forms with adequate forethought. Staff training and information technology systems should be designed so that the original constraints on using a piece of personal information are remembered and respected.

9. **The Legalistic Trap:** An enterprise falls into the legal trap when it focuses solely on meeting the minimum technical demands of the law, and overlooks the value of satisfying the privacy expectations of potential customers and employees. Being seen as "privacy safe" can be good business, and the formulation and marketing of privacy policies should be crafted with this in mind. Businesses can adopt strategies such as making themselves compliant with the federal law even before it technically applies to them, having themselves certified as

"privacy safe" by independent agencies, and by explaining and publicizing their privacy policies in an appealing manner.

10. **The File Trap:** Depending upon how it is interpreted, PIPEDA might apply to many data-gathering exercises beyond adding to written files. These practices may include employee drug testing or monitoring employee phone calls and emails. To the extent that PIPEDA does not govern these practices, other branches of privacy law – such as Manitoba's Privacy Act– may still apply. Businesses should adopt privacy policies and systems that address the whole range of privacy issues from both legal and marketplace considerations. Focusing on the compilation and management of data files is not enough.

11. **The "Best Before Date" Trap:** PIPEDA provides that a business cannot retain personal information for longer than is reasonably necessary. Businesses should have in place systems whereby information is reviewed and deleted as it becomes obsolete or as the original consent pertaining to it expires.

12. **The Security Trap:** The failure to take adequate security measures to protect personal data may amount to non-compliance with the new federal privacy statute. Information must be protected from third party attacks as well as from leaks by a business' own staff. Systems for the physical and electronic storage of data, and access to it, must be designed with security in mind.

13. **The "Words, Not Deeds" Trap:** It is not enough to issue pronouncements as to how a business intends to respect privacy. Personnel training and the design of information technology systems must ensure that operational realities actually live up to paper promises. Businesses may find it useful to conduct internal audits and tests in this respect.

14. **The "Four Corners of the Federal Statute" Trap:** A business may aim to comply with the federal statute but fail to pay adequate attention to other branches of privacy law that continue to be fully in force. Privacy requirements can arise from contract law, labour law, tort law, human rights regimes, general privacy regimes such as the Manitoba Privacy Act, and specialized regimes like the Bank Act. Systems and personnel should be structured so as to address all relevant legal concerns simultaneously. Privacy officers should be trained and instructed to keep an eye on many fronts rather than focusing exclusively on the new federal privacy statute.

15. **The Duty to Disclose Trap:** In some contexts, such as compliance with federal money laundering and anti-terrorism statutes, a business may have a statutory duty to report suspicious or illegal transactions. A business' customers and employees may not be aware of such requirements. As a result, they may feel betrayed when disclosure takes place. The privacy policy statements and consent forms of a business should contain the appropriate warnings. Information technology systems should be designed so as to comply with reporting laws as well as privacy laws.