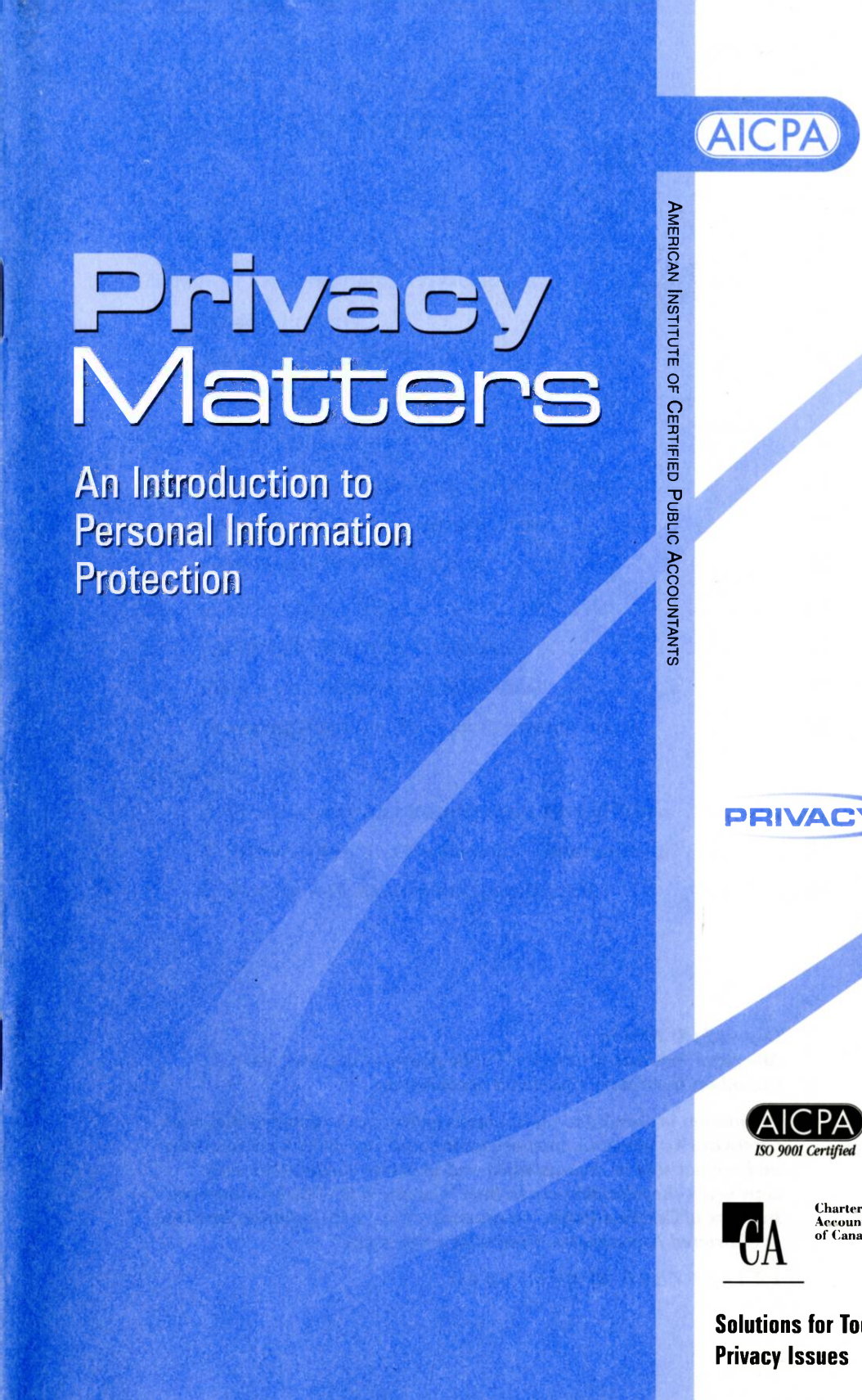
2003

privacy matters: an introduction to personal information protection

American Institute of Certified Public Accountants

Chartered Accountants of Canada


AICPA
American Institute of Certified Public Accountants
Privacy Matters
An Introduction to Personal Information Protection
PRIVACY
AICPA
ISO 9001 Certified
CA
Chartered Accountants of Canada
Solutions for Today's Privacy Issues

1 2 3 4 5 6 7 8 9 0 MI 0 9 8 7 6 5 4 3

TABLE OF CONTENTS

Introduction

> Privacy encompasses the rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention of personal information. Personal information is any information that is or reasonably could be attributable to a specific individual.

Privacy matters! In fact, one of today's key business imperatives is maintaining the privacy of personal information. As business systems and processes become increasingly complex and sophisticated, more and more personal information is being collected. As a result, personal information may be exposed to a variety of vulnerabilities, including loss, misuse, and unauthorized access and disclosure. Those vulnerabilities raise concerns for organizations, the government, and the public in general.

Organizations are trying to strike a balance between the proper collection and use of their customers' personal information. The government is trying to protect the public interest but, at the same time, manage its own cache of personal information gathered from citizens. Consumers are very concerned about their personal information and believe they have lost control of it. With identity theft on the rise, and fears of financial or medical records being accessed inappropriately, there is a pressing need to protect personal information. To address these concerns, a myriad of laws and regulations are being debated and enacted at both the national and state levels of government in the United States, Canada, and elsewhere around the world with the goal of protecting personal information. In addition, nongovernmental organizations, like the Organisation for Economic Co-operation and Development (OECD) and the European Union (EU), are striving for uniformity and standards regarding the management of personal information.

Privacy is a risk management issue for all organizations, and many are looking for privacy solutions. Certified public accountants and chartered accountants (CPAs/CAs) are adept at performing comprehensive risk assessments for businesses and developing risk management solutions that offer competitive marketplace advantages. Research shows they have the skills to implement effective privacy programs in any organization—no matter how big or small. They understand business processes, how information flows within an organization, and how to design effective privacy control systems.

The purpose of this guide is to raise awareness and understanding about privacy matters. First, it defines privacy and explains the importance of protecting personal information, identifies concerns over inadequate privacy protection, and highlights the benefits of good privacy practices. Second, it presents an overview of privacy laws, explains why information privacy is a risk management issue, and discusses how to design a privacy program. Third, it describes internationally recognized fair information practices and the role they play in managing privacy risk—online or offline. Finally, it explains the joint AICPA/CICA Enterprise-Wide Privacy Task Force initiatives to provide business solutions to today's privacy issues by building a Privacy Practices Framework that incorporates concepts from all significant domestic and international privacy laws, regulations, and guidelines.

CHAPTER 1
UNDERSTANDING PRIVACY

This chapter defines *privacy* and explains the importance of protecting personal information. It identifies concerns over inadequate privacy protection and highlights the benefits of good privacy practices.

What Is Privacy?

Privacy has long been regarded as a basic human right in democratic societies.[1] In 1948, the United Nations General Assembly issued the *Universal Declaration of Human Rights*. Article 12 of that declaration states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Privacy is "the right to be left alone."[2] It is "freedom from intrusion or public attention."[3] It concerns our right to control the flow of information about ourselves, the right to fair, reasonable, and confidential practices. A reasonable expectation of privacy might encompass:

- Personal privacy (for example, physical and psychological privacy)
- Privacy of communication (for example, freedom from monitoring and interception)

1 The evolution of privacy is discussed in *Perspectives on Privacy*, a booklet published by the Royal Bank Financial Group.

2 The modern formulation of the concept of privacy was stated in an article by two American jurists. Samuel Warren and Louis Brandeis. The Right to Privacy. *Harvard Law Review*, 1890, p. 193.

3 *The Concise Oxford Dictionary of Current English.* 1990. Oxford: Clarendon Press.

- Privacy of information (for example, control over the collection, use, and disclosure of personal information by others)

This guide focuses on the privacy of personal information. *Privacy* encompasses the rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention of personal information. *Personal information* is information about an identifiable individual that includes any factual or subjective data, recorded or not, in any form. Personal information might include, for example:

- Name, identification numbers, address, income, or hair color
- Evaluations, comments, credit history, or driving records
- Employee files, credit records, loan records, or the existence of a dispute between a consumer and a merchant

Certain personal information is considered sensitive and therefore prone to abuse if handled improperly. *Sensitive personal information* might include, for instance, information on medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and sexual preferences.

Privacy Versus Confidentiality?

Privacy, as defined by laws and regulations, is about individuals having control over the collection, use, disclosure, and retention of their personal information. Unlike privacy, there is no widely accepted definition of *confidentiality* but, in most cases, it is about keeping business information from being disclosed to unauthorized parties, and it is usually driven by agreements or contractual arrangements.

It is important to understand that privacy is about individuals having control over their personal information. In this context, control means individuals have fundamental *rights*, including:

- Knowing what personal information is collected, how it is used, and to whom it is disclosed
- Accessing personal information and correcting inaccuracies
- Challenging decisions made on the basis of inaccurate or incomplete data

Individuals often forget that they have *obligations* concerning privacy; in other words, privacy is a two-sided issue, and is not just about individuals' *rights* to have their personal information protected. As consumers, individuals are obligated to take an active role in managing their personal information, such as deciding whether to provide their personal information to an organization for marketing purposes or taking steps to correct errors in their credit reports.

Protecting the privacy of personal information imposes certain *obligations* on organizations as well. Such obligations prohibit organizations from collecting, using, disclosing, or retaining personal information without the knowledge and consent of individuals.

Why the Concern?

Privacy as an *issue* is not new. It has been debated, argued, and even legislated for decades.[4] This debate is not limited to the real world. Privacy was a pivotal theme in George Orwell's novel, *1984*, and films such as *Minority Report* and *Gattaca* have tackled issues surrounding the privacy of personal information. Research studies show that consumers are feeling frustrated about privacy. In a recent study conducted for Privacy & American Business by Harris Interactive (sponsored by the AICPA and Ernst & Young), 79 percent of consumers said they have lost all control over how companies collect and use their personal information.[5]

4 The Privacy Act of 1974 was passed to control how U.S. government agencies gather and use personal information of U.S. citizens.

5 Similarly, a study by the National Federation of Independent Business (NFIB) Research Foundation, *National Small Business Poll—Privacy*, found that U.S. small business owners are concerned about the unauthorized collection, release, and use of both their business and personal information; 81 percent of those worried about privacy do not distinguish between the two.

Privacy is also a global issue! Many countries have adopted privacy legislation governing the domestic use of personal information, as well as the export of such information across borders and, in particular, to countries that have not adopted similar privacy protection legislation.[6] The United States has often taken a different approach by enacting privacy legislation that applies to specific industries, including the financial and health sectors.

Apart from the legislation, other drivers affecting privacy include advocacy groups, the privacy rights movement, voluntary industry privacy codes, and the public expectation that, as governments adopt freedom of information legislation to provide greater public access, so too should the private sector. Furthermore, these expectations are increasing as the public becomes more aware of privacy issues—such as identity theft—through media reports, presentations, and professional publications. These rising expectations are placing additional demands to address these concerns on all organizations.[7]

Good Privacy Practices Make Good Business Sense

Good privacy practices can provide a consistent approach to protecting personal information in a way that individuals can easily understand and organizations of all sizes, across all industry sectors, can readily implement. They permit flexibility in meeting business needs, limit administrative costs to those directly associated with implementing privacy programs within the organization, and encourage individuals to address the organization first to resolve complaints. In addition, they promote the growth of e-commerce by establishing an enforceable and consumer-friendly privacy environment.

From a business perspective, the benefits of good privacy practices include:

6 Privacy International and the Electronic Privacy Information Center annually review privacy laws in over 50 countries around the world. The 2002 survey is available online (www.privacyinternational.org/survey/).

7 For information on identity theft, see the U.S. government's central Web site (www.consumer.gov/idtheft).

- Protecting the organization's public image and brand
- Protecting valuable data on the organization's customers
- Achieving a competitive advantage in the marketplace
- Meeting the requirements of an industry association
- Efficiently managing personal information and, thereby, reducing administration costs and avoiding unnecessary financial costs, such as retrofitting information systems
- Enhancing credibility and promoting continued consumer confidence and goodwill

Good privacy practices can do far more than build consumer confidence and protect the integrity of an organization's brand—they can also increase customer loyalty and add to the bottom line. According to the recent Harris Interactive Study for Privacy & American Business, almost 50 percent of consumers said they would buy more frequently and in greater volume from companies known to have more reliable privacy practices.

Many organizations may not have given much thought to using privacy protections to promote consumer confidence and goodwill. For the most part, privacy is considered a legal compliance matter instead of a customer-strategy matter. However, the way personal information is obtained and used is both a challenge and an opportunity for businesses. Although the "privacy culture" is changing slowly, privacy is still a largely untapped customer-building resource in most businesses.

Just as good privacy practices have a positive impact on business, not having good privacy practices in place can increase risk to an organization. The Privacy & American Business Study indicates that 83 percent of consumers would stop doing business entirely with companies that misuse customer information.[8]

8 According to a recent report by Jupiter Research, companies that fail to post and support clear privacy policies may be leaving money on the table. As much as $24.5 billion in online sales alone will be lost by 2006 because companies do not adequately address consumers' privacy and security apprehensions.

The misuse of customer information can potentially result in the following:

- Damage to an organization's reputation, brand, and business relationships
- Charges of deceptive business practices
- Customer, employee, and stockholder distrust
- Reduced revenue, market share, and shareholder value
- Refusal by customers to consent to the use of personal information for business purposes
- Legal liability and industry or regulatory sanctions

Clearly, an organization that follows good privacy practices will not only avoid potential legal liability and sanctions, but will likely satisfy both domestic and international requirements to protect personal information. In this regard, many European countries do not allow the transfer of personal information to an organization outside the country unless that organization has adequate privacy protection practices. An overview of domestic and international privacy laws, regulations and guidelines is presented in Chapter 2, "Implementing a Privacy Program," herein.

CHAPTER 2
IMPLEMENTING A PRIVACY PROGRAM

This chapter presents an overview of privacy laws, explains why information privacy is a risk management issue, and discusses how to design a privacy program based on international principles of fair information practices.

Privacy Laws, Regulations, and Guidelines

For the many reasons set out in Chapter 1, "Understanding Privacy," protecting the privacy of personal information is crucial! In the United States, that protection is afforded by privacy laws, such as the *Gramm-Leach-Bliley Act* (GLBA) for the financial services industry, the *Health Insurance Portability and Accountability Act* (HIPAA) for the health care industry, and the *Children's Online Privacy Protection Act* (COPPA) for protecting minors on the Internet. Appendix A, "Privacy Laws and Regulations—United States," to this guide reviews these and other policy privacy developments in the United States.

Other important laws and guidelines include

- The OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*
- The EU's *Data Protection Directive*
- The U.S. Department of Commerce's *Safe Harbor Agreement*
- Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA)
- The United Kingdom's *Data Protection Act*

Appendix B, "Privacy Laws and Regulations—International," to this guide reviews international policy developments.

The recent activities of regulatory bodies indicate a growing trend to publish actions taken against organizations that misuse personal information. For example, the Web sites of the U.S. Federal Trade Commission (FTC) and the Canadian Federal Privacy Commissioner both provide details of corporate privacy violations; findings of regulators; and fines, penalties, or other retribution. In this respect, the FTC reports that fines for privacy violations can easily reach the seven-figure range. As a result, entities that treat consumer data with nonchalance can incur huge legal headaches and public relations nightmares. Such regulatory activities provide evidence of the increasing risk to organizations that choose to ignore personal information privacy.

Privacy Is a Risk Management Issue

Information privacy is a significant concern to many individuals. Numerous surveys and polls in the United States have identified fears about the security and privacy of personal information as a major factor in limiting the growth of commerce on and off the Internet. As such, privacy is a risk management issue for all organizations today—whether online or offline.

Management has always been responsible for managing risk. Information privacy adds to those risks and must be addressed in a timely and complete manner to ensure the requirements of laws, regulations, and industry practices are included in the solution.

Protecting the privacy of personal information presents management with a number of risks to be addressed, including:

- *Image and Branding.* Breaches in privacy protection have the potential to negatively affect an organization's image and brand, and hence how it is perceived in the marketplace.
- *Financial Loss.* Significant financial losses may result from breaches of privacy protection, either directly (for example, the cost of reissuing credit cards) or indirectly (for example, lost customer loyalty and sales).

- *Investor Loss.* The marketplace may react to breaches in privacy protection by driving down share prices, resulting in a loss of market capitalization.
- *Regulatory Compliance.* Failing to comply with regulatory requirements may result in poor public relations, as well as fines or other penalties.
- *Business Partner Confidence.* Business partners that share personal information but fail to adequately protect that information may suffer a loss of confidence and trust.
- *International Agreements.* When an organization cannot meet established privacy standards, certain international privacy laws may restrict or prohibit the export of personal information to that organization.

To determine the significance of privacy-related business risks, it is important for every organization to conduct a risk assessment of its information-handling practices. The results of that assessment will dictate whether and to what extent a privacy program should be implemented. Prudent business practices call for a privacy risk assessment either as part of an initial privacy review or when major changes are being proposed to existing business activities. Generally, activities that involve the significant collection, use, or disclosure of personal information should include such an assessment and the results should be reflected in the organization's business plan. Appendix C, "Privacy Risk Assessment Questionnaire," to this guide sets out key questions that should be addressed as part of an initial privacy risk assessment.

An effective privacy program requires clear leadership and a commitment by business owner/managers or senior management to prevent, detect, and address noncompliance. Accordingly, those assigned responsibility for privacy compliance must be given the decision-making authority to oversee the organization's privacy practices, including the implementation of policies and procedures, staff training, allocation of resources, dissemination of information, and response to and resolution of inquiries and complaints. Business owner/managers or senior management must also ensure that adequate resources are available for designing

the privacy program, and the time frame for implementation should be realistic.

Designing a Privacy Program

Any organization that has a well-designed, well-implemented, and well-monitored privacy program will not only respond to the concerns of consumers but will also comply with the applicable privacy laws. Because the nature, size, and complexity of operations will vary from one organization to another, a privacy program should be tailored to meet the needs of the particular organization. In most cases, this means using the following road map for protecting the privacy of personal information.

Road Map for Protecting the Privacy of Personal Information

1. **Appoint** an individual to be responsible for privacy compliance throughout the organization and managing personal information shared with business partners.
2. **Inventory** current privacy practices, identifying all sources, uses, locations, sharing, disclosure, archiving, and destruction of personal information.
3. **Assess** the gaps between the organization's current privacy practices and fair information practices, including pertinent privacy laws, regulations, and guidelines.
4. **Prepare** privacy policies and procedures to effectively address all fair information practices and pertinent legal requirements.
5. **Appoint** a cross-functional team, as needed, to develop a detailed change management plan and make the required changes.
6. **Implement** the privacy program with respect to policies, procedures, information systems, contracts, and other privacy-related materials.
7. **Monitor** and report on compliance with the organization's privacy policies and procedures in accordance with fair information practices.

Step 1 in the preceding road map is to delegate the responsibility for the protection of personal information to one individual—often called a *privacy officer*. This step is crucial because it formally establishes a "custodian" or "trustee" to serve as the intermediary between individuals who provide personal information and those who use that information, whether they are internal staff or third parties. Assigning responsibility to a privacy officer provides a means for building expertise in effectively managing privacy issues relating to any of an organization's operations.

According to a study undertaken jointly by Privacy & American Business and the Association of Corporate Privacy Officers, 82 percent of privacy officers report directly to senior officials and 78 percent have backgrounds in privacy-related functions, such as legal, public, or government affairs; marketing; information technology; or management. Whatever the size of the organization, the privacy officer should have an understanding of people, processes, and technology that must include the following:

- A broad understanding of how the organization works and its corporate culture
- A positive track record of working with cross-functional teams
- Strong interpersonal, communications, and leadership skills
- Technical savvy about data management and computer systems

It is important to communicate the name, title, and responsibilities of the privacy officer, both internally and externally, for example, in published materials, such as privacy manuals and brochures, and on Web sites. The responsibilities will differ from one organization to another but, at a minimum, the privacy officer will need to determine whether the systems that store personal information have the capacity to track and record who has access to that information, and for what purpose and under what conditions the information is used. As well as ensuring that the staff is adequately trained, the privacy officer should determine

whether personal information is disclosed to third parties, and how they are contractually bound to protect privacy.

Step 2 of the preceding road map is to inventory current privacy practices. In this regard, the privacy officer should identify all personal information-handling practices, including ongoing activities and new initiatives. A checklist may help to create the inventory by asking questions such as:

- What personal information is collected?
- Why is it collected?
- How is it collected?
- What is it used for?
- Where is it kept?
- Who has access?
- What security measures are used?
- To whom is it disclosed?
- When and how is it disposed of?

After completing the inventory, the privacy officer follows step 3 of the road map, which it to assess the gaps between the organization's current privacy practices and fair information practices, including pertinent privacy laws, regulations, and guidelines. In step 4, he or she prepares privacy policies and procedures in accordance with internationally recognized fair information practices. (Herein, Chapter 3, "Managing Privacy Risk," provides initial guidance for such an undertaking.)

Upon the completion of the preparation of policies and procedures, step 5 is carried out, as needed. A cross-functional team is appointed to develop a detailed change management plan and make the required changes.

Steps 6 and 7 of the road map to compliance address risk management—implementation and monitoring of the privacy program with respect to policies, procedures, information systems, contracts, and other privacy-related materials. In this regard, it is important to understand that privacy risk management is a continuous, evolving process

that is relevant to all facets of the business. That process encompasses the following approach:

- Identify the pertinent fair information practices. (Refer to Chapter 3.)
- Establish specific objectives.
- Identify and assess risks of not meeting the objectives.
- Identify and implement appropriate control measures.
- Assess the effectiveness of control measures.

An organization should establish specific objectives with respect to each fair information practice. Risk identification and assessment will provide a basis for understanding the risks that may prevent those objectives from being met. Control identification and assessment will provide the means for mitigating risks, achieving the objectives and in turn complying with the fair information practices. In this regard, it is crucial for management to identify the consequences of not meeting the established objectives and specify the control measures needed to prevent unacceptable risks, manage and monitor acceptable risks, and mitigate unexpected risks.

CHAPTER 3
MANAGING PRIVACY RISK

This chapter describes fair information practices and the role they play in managing privacy risk—on and off the Internet. It also explains the AICPA/CICA Privacy Task Force initiatives to provide business solutions to today's privacy issues.

About Fair Information Practices

Internationally recognized fair information practices have been developed by experts worldwide as models for protecting the privacy of personal information and managing privacy risk. At a minimum, fair information practices call for the following actions:

1. *Notice.* The entity provides notice about its privacy policies and practices to the individual and identifies the purpose for which personal information is collected.
2. *Choice and Consent.* The entity describes the choices available to individuals and obtains implicit or explicit consent from the individual with respect to the collection, use, disclosure, and retention of personal information.
3. *Collection.* The entity limits the collection of personal information to the purposes described in the notice.
4. *Use and Retention.* The entity limits the use of the personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary for the fulfillment of the stated purposes, or as required by laws or regulations.

5. *Access.* The entity provides access to the individual to review and update their personal information.
6. *Onward Transfer and Disclosure.* The entity discloses personal information to third parties for the purposes identified in the notice and for which the individual has provided implicit or explicit consent as permitted by laws or regulations.
7. *Security.* The entity takes reasonable precautions to protect personal information.
8. *Integrity.* The entity maintains accurate, complete, and relevant personal information for the purposes for which it is to be used.
9. *Management and Enforcement.* The entity establishes accountability for and monitors compliance with its privacy policies and has procedures to address privacy-related inquiries and disputes.

The following guidance examines these nine fair information practices in terms of the rights of the individuals and the obligations of organizations. For each, the objectives and related risks are highlighted and specific privacy requirements are explained.

Notice

This fair information practice acknowledges that an organization should make specific information about its privacy policies and procedures readily available to individuals. An organization must ensure that individuals obtain the information they need to make informed decisions about their business relationship with the organization. Various risks are associated with the failure to meet these objectives. For example, if an individual cannot readily determine an organization's privacy policies, trust and confidence will be undermined, resulting in the denial of consent to use personal information for business purposes.

Notice requires that an organization openly communicate to both employees and customers their policies and procedures for the management of personal information. To meet their responsibilities, it is important for employees to

be aware of and understand procedures for responding to individual inquiries, including those related to:

- The name and title of the person accountable for the organization's privacy program
- The name, title, and address of the person to whom access requests should be sent
- How individuals can access their personal information
- How individuals can file a complaint with the organization

In addition, an organization should inform individuals why it is collecting information about them (e.g., to provide benefits to employees, open an account, verify creditworthiness, or process a subscription). An organization is not allowed to mislead individuals about the reasons for collecting personal information. Furthermore, individuals should be informed as to how to contact the organization regarding any inquiries or complaints; any third parties to which personal information may be disclosed; and the choices and means for limiting the collection, use, and disclosure of their personal information. Various risks are associated with the failure to meet these objectives. For example, misrepresenting the purpose for collecting personal information may give rise to charges of deceptive business practices.

Choice and Consent

This fair information practice acknowledges the right of individuals to be provided with clear, conspicuous, readily available, and affordable mechanisms to exercise choice. An organization is obligated to inform and obtain permission from individuals before collecting or using their personal information for the purpose specified in the notice. If personal information is to be disclosed to a third party or used for a purpose other than that specified in the notice, individuals should be given the opportunity to voluntarily choose (*opt-in* or *opt-out*) whether or not to allow such disclosure or alternative use.

For *sensitive personal information* (e.g., information on medical or health conditions), individuals normally must

give affirmative or explicit (opt-in) consent if their information is to be disclosed to a third party or used for a purpose other than for which it was originally collected or subsequently authorized by the individual. In any case, any information received from a third party, if the third party treats and identifies it as sensitive, should be treated by the organization as sensitive personal information.

Various risks are associated with the failure to meet these objectives. For example, an organization that fails to obtain consent from individuals before collecting, using, or disclosing their personal information may be subject to legal liability or sanctions, particularly if the obligation to seek consent is required by law. Furthermore, if consent is not obtained, or is obtained in ways inappropriate to the sensitivity of the personal information, the organization's reputation may suffer, customer trust may be eroded, and customers may withdraw consent for the future use of their personal information. (There are some exceptions, however. Special cases are set out below with respect to situations in which an organization may collect, use, or disclose personal information without the knowledge or consent of an individual.)

Collection

As a general rule, this fair information practice precludes an organization from collecting personal information indiscriminately. Various risks are associated with the failure to meet the objective. Gathering more information than necessary may expose the organization to greater liability and security risks. In addition, it may raise the administrative costs of collecting and retaining the data, and increase the risk of inappropriate use and disclosure.

There are some exceptions to the general rule. An organization may *collect* personal information without the knowledge or consent of an individual under any of the following circumstances:

- The collection is clearly in the interests of the individual and consent cannot be obtained in a timely way.
- It is reasonable to expect that the collection with the knowledge or consent of the individual would com-

promise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of federal or state laws.

- The collection is solely for journalistic, artistic or literary purposes.
- The information is publicly available.

Use and Retention

As a general rule, this fair information practice precludes an organization from using personal information for other than the purposes specified in the notice, except with the explicit consent of the individual. It also precludes an organization from retaining personal information after the specified purposes are fulfilled.

Various risks are associated with the failure to meet the objectives. The unauthorized use of personal information can jeopardize customer trust and result in legal liability or sanctions. If a minimum retention period is not specified, personal information may be destroyed prematurely, making it unavailable for decision-making purposes. If a maximum retention period is not specified, personal information may become inaccurate over time. It may also be difficult to manage and increase the administrative costs of storing and archiving the data.

The following are exceptions to the general rule whereby personal information may be *used* without an individual's knowledge or consent:

- The use is clearly in the individual's interest and consent is not available in a timely way.
- Knowledge and consent would compromise the availability or accuracy of the information, and collection was required to investigate a breach of an agreement or contravention of a federal or state law.
- The organization has reasonable grounds to believe the information could be useful when investigating a

contravention of a federal, state, or foreign law and the information is used for that investigation.

- An emergency threatens the individual's life, health, or security.
- The information is being collected for statistical or scholarly study or research.
- The information is publicly available.

Access

This fair information practice acknowledges the right of individuals to access their personal information held by an organization and to be provided with the means to review, update, block the further use of, or permanently erase that information. A corresponding obligation is imposed on the organization to facilitate the individual's access rights on request. There are exceptions if the burden or expense of providing access would be disproportionate to the risks to the individual's privacy or if the rights of persons other than the individual would be violated. In such cases, the individual should be given an explanation of why he or she is being denied access.

Typically, a request should be in writing and an organization should provide assistance, as needed, in preparing the request. A fee may be charged by the organization only if it has informed the individual of the approximate cost and the individual does not withdraw the request. In addition, an organization should respond to a request with due diligence and, in any case, usually not later than 30 days after receiving the initial request. An organization that responds within the time limit and refuses a request should inform the individual in writing of the refusal, setting out the reasons and any recourse available. An organization with personal information that is the subject of a request must also retain that information for as long as it is necessary to allow the individual to exhaust any recourse available.

In some situations, an organization may not be able to provide access to all the personal information it holds about an individual. The reasons for denying access should be pro-

vided to the individual, on request. Exceptions may include information that:

- Is prohibitively costly to provide.
- Contains references to other individuals.
- Cannot be disclosed for legal, security or commercial proprietary reasons.
- Is subject to attorney-client or litigation privilege.

In certain circumstances, a request for access can be legally denied, for example, giving an individual access to personal information that would reveal personal information about a third party. If that information is severable, the organization should delete the information about the third party before giving the individual access. This would not apply if the third party consents to the access or the individual needs that information because an individual's life, health, or security is threatened.

Access to personal information may also be restricted because it relates to investigations of offences or national security, or as a result of any of the following:

- The information is protected by attorney-client privilege.
- To give access would reveal confidential commercial information.
- To give access could reasonably be expected to threaten the life or security of another individual.
- The information was collected with respect to investigating a breach of an agreement or a contravention of a law.
- The information was generated in the course of a formal dispute resolution process.

Onward Transfer and Disclosure

As a general rule, this fair information practice acknowledges the right of individuals to be notified that personal information may be disclosed to third parties and to volun-

tarily choose (opt-in or opt-out) whether such information will be disclosed to a third party or used for a purpose that is other than that described in the notice, except as permitted by laws or regulations. A corresponding obligation is imposed on the organization to disclose personal information only to third parties who provide substantially equivalent protection to such personal information, and according to the specific notice and choice practices disclosed to the individual. Further transfers of the personal information by the third party should be permitted only if the transfer is also subject to practices affording an adequate level of protection.

Personal information may be *disclosed* without the individual's knowledge or consent to:

- Assist a lawyer representing the organization.
- Collect a debt the individual owes to the organization.
- Comply with a law, subpoena, warrant, or order made by a court or other body with appropriate jurisdiction.
- Assist a government institution requesting the information under lawful authority and indicating that disclosure is for the purpose of:
  - Conducting an investigation, or gathering intelligence relating to any federal, state, local, or foreign law.
  - Protecting national security or conducting international affairs.
  - Administering any federal or state law.
- Assist an investigative body for the purposes related to the investigation of a breach of an agreement or a contravention of a federal, state, or local law.
- Resolve an emergency threatening an individual's life, health, or security.
- Assist in the compilation of a statistical study, scholarly study research, or the work of an archival institution.

Security

This fair information practice acknowledges that organizations creating, maintaining, using, or disseminating personal information should take reasonable precautions to protect it from loss, misuse, unauthorized access or disclosure, alteration, and destruction. Personal information should be protected by safeguards (physical, organizational, and technological measures) that are appropriate to the sensitivity and value of the information.[9]

Various risks are associated with the failure to meet these objectives. For example, if appropriate security measures are not in place, unauthorized parties may be able to access and use, copy, disclose, alter, or destroy personal information. Significant harm could be done to individuals whose personal information is compromised, and the organization responsible for protecting that information could be held liable. Therefore, the more sensitive the information (for example, financial or medical data), the greater the potential harm and the need for increased security.

Integrity

This fair information practice acknowledges that an organization should maintain accurate, complete, current, relevant, and reliable personal information for the purposes for which it is to be used. Personal information should be updated only when necessary to meet the identified purpose.

Various risks are associated with the failure to meet these objectives. For example, an individual might be harmed by the use or disclosure of inaccurate data. If an organization uses inaccurate or misleading personal information to make business decisions, customer relations may be jeopardized, resulting in lost profits and market share.

9 For example, consumers demand that Internet transactions be protected. Public key infrastructure (PKI) and digital certificates are important safeguards. PKI is the framework that protects the data, using specialized encryption software and associated policies and services. PKI uses numeric keys to enhance security. Digital certificates (a kind of identification card that authenticates their holder's ID) are used by certification authorities as a type of Internet passport.

Management and Enforcement

This fair information practice acknowledges that an organization should be responsible for the protection of personal information. In this respect, an organization should designate one or more individuals who are accountable for the organization's compliance with its stated privacy policies and for procedures to address privacy-related inquiries and disputes. Therefore, a privacy officer should be appointed to oversee privacy compliance and to implement policies and procedures that apply to all personal information under the organization's control, including transfers to third parties.

Various risks are associated with the failure to meet these objectives. For example, in the absence of an effective accountability regime, personal information may be mismanaged, resulting in potential damage to the organization's reputation and business relationships. In addition, if an individual cannot readily determine an organization's privacy policies, or procedures for raising privacy-related inquiries, trust and confidence will be undermined, resulting in the denial of consent to use personal information for business purposes. Furthermore, the inability to satisfactorily respond to inquiries and complaints could lead to potential loss of business and have a negative effect on the organization's compliance with pertinent privacy laws, regulations, and guidelines.

This fair information practice also acknowledges the right of individuals to challenge an organization's compliance with stated privacy policies and procedures. An organization is obliged to provide the means by which an individual can exercise that right. This includes explaining the organization's procedures and the various avenues of recourse available to the individual. Accordingly, it is important that the privacy officer develop easily accessible complaint procedures and inform complainants of avenues of recourse, including those of industry associations and regulatory bodies. To meet these responsibilities, the privacy officer (or a designated employee) would investigate all complaints received, taking care to record the date a complaint is received and the nature of the complaint, and acknowledge receipt of the complaint promptly. If necessary, the individual would be contacted to clarify the complaint.

Normally, the investigation would be assigned to a person with the skills necessary to conduct it fairly and impartially, and the investigator would be given access to all relevant records, employees, or others who handled the personal information or access request. The investigator would notify the individual of the outcome of the investigation, explaining any relevant steps taken. Any inaccurate personal information would be corrected and/or policies and procedures would be modified based on the outcome of the investigation.

Various risks are associated with the failure to meet these objectives. For example, individuals may make inquiries or lodge complaints on personal information matters such as delays in responding to a request, incomplete or inaccurate responses, improper collection or use, and improper disclosure or retention of that information. If an organization does not have an effective process for addressing such inquiries and complaints, individuals will not be able to assess how well their personal information is managed. This could destroy customer confidence, resulting in customer dissatisfaction and lost business.

Online and Offline—It's Still Privacy

Since 1997, the concept of online privacy has been hotly debated by a slew of consumer privacy advocacy groups that were awakened by new threats from the then-nascent Internet. In the few short years since then, as Internet use has exploded exponentially, the Web has become more familiar to consumers. Consumer advocacy groups are on the front lines battling companies that have violated consumer privacy or followed poor Internet privacy practices. Businesses with an online presence are under close scrutiny by many organizations, including watchdogs, regulators, and legislators, following how they collect and use their customers' personal information.

WebTrust for Online Privacy was developed by the AICPA and CICA to meet a very specific need for e-commerce businesses. As organizations address personal information about their customers or employees, they need to consider all of the privacy issues surrounding that information.

Many organizations have turned to the accounting profession for privacy solutions. They are looking for help in developing good privacy practices throughout the organization and demonstrating to their customers that they manage personal information properly.

The business community is now asking for something broader in scope than just online privacy guidelines—they are looking for total, enterprise-wide privacy solutions. As the global economy evolves and information flows become borderless, organizations need solutions to help them manage those information flows effectively.

The goal is to have an integrated privacy program, instead of separate privacy policies and procedures for the Privacy Act of 1974, the GLBA or the HIPPA, and for online and offline. Clearly, it is in the public interest to have comprehensive privacy practices. It also is in the best interest of every organization that interacts with the public.

Providing Solutions to Today's Privacy Issues

Most organizations recognize that good privacy practices are central to corporate governance and accountability. It is acknowledged, however, that some organizations will do the minimum required to protect personal information and still comply with the law. Some can be coaxed to "do the right thing" and protect the privacy of their customers. Many others will see how privacy can be used as a competitive advantage. Whatever the motivation, businesses are looking for guidance and assistance in managing privacy risk. Each of these scenarios includes the CPA/CA, a trusted business adviser who is skilled at examining management information systems and adept at identifying the controls needed to effectively manage risk.[10]

Many members of the accounting profession are actively helping businesses develop and implement sound privacy

10 A study by the NFIB Research Foundation, *National Small Business Poll—Advice and Advisors*, found that 74 percent of owners employing 20 or more people sought advice from their accountant and 83 percent took that advice.

programs. Building on this expertise, the AICPA and the CICA jointly established an Enterprise-Wide Privacy Task Force comprising a cross section of the accounting profession, including industry, large multinational firms, and small CPA/CA firms, as well as members in academia and the legal profession. Its mission is to examine the role CPAs/CAs can play in advising organizations about privacy issues and risks, and to develop a privacy framework that will serve as a benchmark for good privacy practices.

The Privacy Task Force is developing a Privacy Practices Framework that can be used by all CPAs/CAs (both in industry and in public practice) to guide and assist the organizations they serve in implementing privacy programs using a standard set of privacy best practices. This framework incorporates concepts from all significant domestic and international privacy laws, regulations, and guidelines. It is the intellectual capital and body of knowledge around which all other privacy advisory and assurance services can be built.

Research shows that CPAs/CAs have all the skills necessary to implement effective privacy programs in any organization—no matter how big or small. They understand business processes, how information flows within an organization, and how to design effective privacy control systems. Through a wide range of advisory and assurance services, CPAs/CAs have an opportunity to help businesses navigate the patchwork of privacy laws, regulations, and guidelines and focus on the heart of the matter—building trust between customers and businesses and "doing the right thing" by following good privacy practices.

CPAs/CAs in public practice will be able to offer clients a full range of services, including strategic and business planning, privacy gap and risk analysis, benchmarking, privacy policy design and implementation, performance measurement, and independent verification of privacy controls. CPAs/CAs in industry can enhance their value to their employers through performing internal assessments against something they can measure—the AICPA/CICA Privacy Practices Framework.

For more information

To learn more about privacy and how implementing new privacy measures can benefit your organization, please visit the Online Center for Privacy Information at

www.aicpa.org
or
www.cica.ca/privacy

APPENDIX A

PRIVACY LAWS AND REGULATIONS—UNITED STATES

This appendix reviews the following information privacy laws in the United States:

The *Privacy Act of 1974* (Privacy Act); and the related *Freedom of Information Act* (FOIA), passed in 1996;

Gramm-Leach-Bliley Act (GLBA) for the financial services industry; the *Health Insurance Portability and Accountability Act* (HIPAA) for the health care industry; and the *Children's Online Privacy Protection Act* (COPPA) for the protection of minors on the Internet.

PRIVACY ACT 1974 AND FREEDOM OF INFORMATION ACT 1966

The *Privacy Act of 1974* (Privacy Act) prohibits federal government agencies from disclosing any personal information about an individual without consent, except in certain circumstances such as law enforcement and census activities. The Privacy Act applies to federal government agencies, as well as businesses that are contractors for a federal government agency and that collect, maintain, process, or transmit data.

In addition to passing the Privacy Act, Congress enacted the *Freedom of Information Act* (FOIA) in 1966. The basic provisions allow individuals to not only access paper documents, but also to access electronically created documents and information, such as electronic databases, electronic documents, word-processing documents, and e-mail. FOIA has broadened the right of individuals to gain greater access to government documents.

GRAMM-LEACH-BLILEY ACT

The *Gramm-Leach-Bliley Act* (GLBA) was passed by Congress in 1999, with an effective date of November 13, 2000. The Provisions in the Act require any financial institution or business that engages in financial activities to provide a privacy notice to their customers by July 1, 2001, and if a relationship is established. The GLBA applies to many types of business, including:[11]

- Lending and extending credit
- Providing financial or investment services
- Insuring, guaranteeing, or indemnifying against loss
- Underwriting or dealing with securities
- Banking or closely related banking services
- Engaging in an activity that a bank holding company may engage in outside of the United States
- Auto dealers that lease or finance
- Appraising real estate or other personal property
- Leasing real or personal property
- Mortgage lenders or brokers

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

The *Health Insurance Portability and Accountability Act* (HIPAA) was passed by Congress in 1996. Organizations must be compliant by April 14, 2003 (April 14, 2004, for small health plans).[12] The act requires health

11 Internet resources include the National Association of Commissioners Guide, Implementing the GLBA Act: One Year Later: Remarks from Governor Meyer to the Federal Reserve Board, PricewaterhouseCoopers GLBA Diagnostic, and An Executive's Guide to U.S. Financial Modernization, Texas Department of Banking, and Perspective from a law firm: Bricker & Eckler LLP.

12 Internet resources include Ernst & Young's HIPAA Resource Center, Pricewaterhouse-Cooper's HIPAA Resources, HIPAA Complete Consulting Firm's Resources, Siemens Health Services HIPAA Central, SciTech Concept EDI HIPAA Compliance Checker, Centers for Medicare & Medicaid Services (formerly known as Health Care Financing Administration) HIPAA resources, and ViPs HIPAA Compliance Solutions.

care providers to meet certain privacy protection standards with respect to personal health information. The protection given must be for both intentional and unintentional disclosures of personal health information. HIPAA applies to the following:

- A *health plan*, defined as an individual plan or group health plan that provides or pays the cost of medical care
- A *health care provider*, defined as a provider of medical or health services and any person or organization who furnishes, bills, or is paid for health care services or supplies in the normal course of business
- A *health care clearinghouse*, defined as a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements

CHILDREN'S ONLINE PRIVACY PROTECTION ACT

The *Children's Online Privacy Protection Act* (COPPA) became effective April 21, 2000. Web sites that are directed to children 12 and under or that "knowingly collect information" from this group must post a notice of their information collection practices that includes:

- The types of personal information they collect from children—for example, name, e-mail, and hobbies
- How the site will use the information—for example, to market and to notify contest winners
- Whether the personal information is forwarded to advertisers or other third parties
- A contact at the site

Businesses that collect data online, even if they do not specifically target children, need to be concerned about whether children in fact visit their sites. Parental consent

must be obtained before collecting data about children 12 and under.[13]

13 Internet resources include the Federal Trade Commission's How to Comply with COPPA and COPPA Links, American Library Association COPPA Guide, and Center for Media Education's Report on COPPA's first year.

APPENDIX B

PRIVACY LAWS AND REGULATIONS—INTERNATIONAL

This appendix reviews international developments on information privacy regarding the Organisation for Economic Co-operation and Development (OECD), the European Union (EU), Canada, and the United Kingdom.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The Organisation for Economic Co-operation and Development (OECD) brings together 30 countries sharing the principles of the market economy, pluralist democracy, and respect for human rights. In September 1980, the OECD developed a set of guidelines for the protection of personal information. The *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (the Guidelines) represent an international consensus on how best to balance effective privacy protection with the free flow of personal data. *Personal data* are defined as "any information relating to an identified or an identifiable individual (data subject)." The OECD's Privacy Guidelines operate on the following basic principles:

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguarding
- Openness
- Individual participation
- Accountability

The Guidelines provide flexibility in applying the principles and allow for various means of compliance.

EUROPEAN UNION

The European Union (EU) is the result of a process of cooperation and integration that began in 1951 among six countries. Today, the EU has 15 member states and is preparing for its fifth enlargement, this time to include Eastern and Southern Europe. As one of its principal tasks, the European Commission (comprising 20 members drawn from the 15 EU countries) ensures the free movement of goods, services, capital, and persons throughout the EU. To create a "frontier free internal market," the European Commission's *Directive on Data Privacy* (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data), was put into effect in October 1998. The Directive imposes obligations on data controllers (anyone responsible for collection, use, or disclosure of personal information) in the public and private sectors and applies to both automated and nonautomated forms of data.

The EU Directive reflects the principles of generally recognized *Fair Information Practices* that form the basis of the OECD Guidelines and most other recognized personal information protection codes. The Directive also seeks to protect the privacy rights of EU citizens if data are transferred beyond EU countries. Article 25 requires that such transfers take place only where the third country "ensures an adequate level of protection" (for example, the U.S. Safe Harbor Privacy Principles). Article 26 contains certain derogations from Article 25, allowing data to be processed in a third country despite the adequacy requirement, if certain conditions are met.

CANADA

In 2000, the Canadian government enacted the *Personal Information Protection and Electronic Documents Act*

(PIPEDA). The PIPEDA, which came into force January 1, 2001, establishes new rules for privacy recognizing the rights of individuals with respect to the collection, use, disclosure, and retention of their personal information. The rules also recognize the obligations of organizations to protect that privacy in a manner that a reasonable person would consider appropriate in the circumstances. Organizations, including corporations, individuals, associations, partnerships, and trade unions, are generally subject to the privacy rules if they collect, use, or disclose personal information in the course of a commercial activity. By January 1, 2004, the privacy rights of all Canadians will be protected in one of two ways—by federal legislation (PIPEDA) or by provincial legislation that is "substantially similar" to the federal legislation.

The PIPEDA establishes Canada as the first country to implement private-sector privacy rules based on national standards, the Canadian Standards Association (CSA) *Model Code for the Protection of Personal Information*. Formally launched in 1996, the CSA Model Code is based on the 1980 OECD guidelines and establishes the following 10 privacy principles to govern the collection, use, and disclosure of personal information:

- Imposing accountability
- Identifying the purposes for the collection of personal information
- Obtaining consent
- Limiting collection
- Limiting use, disclosure, and retention
- Ensuring accuracy
- Providing adequate security
- Making information management policies readily available
- Providing individuals with access to information about themselves
- Giving individuals a right to challenge an organization's compliance with these principles

The Privacy Commissioner of Canada is the ombudsman for complaints under the PIPEDA.[14]

UNITED KINGDOM

The United Kingdom's *Data Protection Act* was approved in July 1998 and came into force on March 1, 2000. It applies to personal data, which includes both facts and opinions about an individual, as well as information regarding the intentions of the data controller toward the individual. Government agencies and private entities processing personal data must comply with the principles of good practice.

The act sets out Data Protection Principles, which, in summary require that personal data must be:

- Processed fairly and lawfully.
- Obtained only for one or more specified and lawful purposes, and not be further processed in any manner incompatible with those purposes.
- Adequate, relevant, and not excessive in relation to the purposes for which they are processed.
- Accurate, up-to-date, and retained only as long as necessary for the stated purposes.

In addition, personal data must be processed in accordance with the rights of data subjects under the act, and appropriate technical and organizational measures must be taken against unauthorized or unlawful processing, accidental loss, destruction, or damage. As well, personal data may not be transferred to a country or territory outside the European economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of subjects in relation to the processing of personal data. Furthermore, entities that collect personal data must register with the Information Commissioner, an independent agency that enforces the act. More than 237,000 data users are registered with the Commissioner.

14 Internet resources include the Canadian Institute of Chartered Accountants' Online Privacy Resource Centre, the Privacy Commissioner of Canada, Information and Privacy Commissioner of Ontario—privacy diagnostic tool, European Union's relations with Canada, and the EU ruling on compliance with Directive 95/46/EC.

APPENDIX C
PRIVACY RISK ASSESSMENT QUESTIONNAIRE

Understanding Privacy

1. What personal information about customers and employees does the organization collect and retain?
2. What personal information is used in carrying out business, for example, in sales, marketing, fund raising, and customer relations?
3. What personal information is obtained from or disclosed to affiliates or third parties, for example, in payroll outsourcing?
4. What is the impact of United States privacy laws and regulations, and/or international privacy requirements, on the organization (which may require a legal interpretation)?
5. How does the organization's business plan address the privacy of personal information?

Implementing a Privacy Program

6. To what degree is senior management actively involved in the development, implementation, and/or promotion of privacy measures within the organization?
7. Has the organization assigned someone (for example, a chief privacy officer) the responsibility for compliance with privacy legislation?

8. Has the designated privacy officer been given clear authority to oversee the organization's information handling practices?
9. Are adequate resources available for developing, implementing, and maintaining a privacy compliance system?
10. What privacy policies has the organization established with respect to the collection, use, disclosure, and retention of personal information?
11. How are the policies and procedures for managing personal information communicated to employees?
12. How are employees with access to personal information trained in privacy protection?
13. Are the appropriate forms and documents required by the system fully developed?

Managing Privacy Risk

14. To comply with the organization's established privacy policies, what specific objectives have been established?
15. What are the consequences of not meeting the specific privacy objectives?
16. To what extent have appropriate control measures been identified and implemented?
17. How is the effectiveness of the privacy control measures monitored and reported?
18. What mechanisms are in place to effectively address failures to properly apply the organization's established privacy policies and procedures?
19. How would the organization benefit from a comprehensive assessment of the risks, controls, and business disclosures associated with personal information privacy?

20. Has the organization considered the value-added services available from an independent assurance practitioner with respect to both offline and online privacy?