The Protection of Personal Information by Charities and Not-For-Profit Organizations: A National Perspective*

M. JASMINE SWEATMAN, B.A., LL.B, TEP, LL.M
O'Connor MacLeod Hanna LLP, Oakville, Ontario

Introduction

Under Canada's *Personal Information Protection and Electronics Documents Act* (PIPEDA):

- if an organization wants to collect, use or disclose personal information about people, it needs consent, except in a few specific and limited circumstances;
- an organization can use or disclose a person's personal information only for the purpose for which that person gave consent;
- even with consent, an organization has to limit the collection, use, and disclosure to purposes that a reasonable person would consider appropriate under the circumstances;
- individuals have a right to see the personal information that the organization holds about them, and to correct any inaccuracies; and
- there is oversight of the legislation through the Privacy Commissioner of Canada to ensure that the law is respected and redress is received if a person's rights are violated.

As a reminder, although the application of PIPEDA expanded in 2004 to commercial activities that normally fall under provincial jurisdiction, it did not extend to employment in those activities. The only place PIPEDA applies to employment is in federal works, undertakings, or businesses.

This evolution has led to a more crystallized approach that lays a principled foundation upon which is built the various Canadian legislation. At times, this evolution explains current thinking and reminds us that the evolutionary process is not over.

*This article is adapted and updated from a presentation at the 2nd National Symposium on Charity Law in Toronto in April 2004. Parts of this article are modified from Jones, P. "Between God and You: Canada's New Privacy Law," published in *The Philanthropist*, Vol. 18, No. 1 (2003), with permission, and from a 2003 presentation by Paul Jones and Jasmine Sweatman.

This article reviews and comments upon the Canadian legislative landscape of privacy protection of the private sector and, in particular, how it may impact upon charities and not-for-profit organizations.[1] The article is divided into three parts. Part I reviews the legislative framework in Canada of these privacy protection statutes. Part II reviews the effect of this legislation on charitable and not-for-profit organizations (except for those in Quebec). And Part III discusses strategies for compliance and remedies. This article does not review or comment upon the protection of personal health information (except for a brief reference to Ontario's Health Information Protection Act, 2004), even though that legislation may have residual impacts on charitable and not-for-profit organizations operating in that sector.

PART I: LEGISLATIVE FRAMEWORK

January 1, 2004, was the deadline for all private sector organizations, corporations, and individuals engaged in commercial activities in Canada to comply with the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) or with designated "substantially similar" provincial legislation.

Since January 1, 2004, PIPEDA protects the collection, use, and disclosure of personal information in the course of any commercial activity in Canada, where there is no provincial legislation in place that is judged substantially similar to the federal law.

The implementation and coming into force of PIPEDA was in three stages. On January 1, 2001, PIPEDA applied to personal information collected, used, or disclosed in the course of commercial activities by federal works, undertakings, and business. On January 1, 2002, PIPEDA was extended to the collection, use, or disclosure of personal health information by those same organizations. Finally, on January 1, 2004, PIPEDA applied to every organization that collects, uses, or discloses personal information, including personal health information, in the course of commercial activities, unless there was in place provincial legislation that has been designated "substantially similar" to PIPEDA. The final determination for this designation rests with the Governor in Council. However, PIPEDA requires the Commissioner to report to Parliament on whether provinces have enacted "substantially similar" legislation and its application.

As of January 1, 2004, three provinces had legislation in force to protect personal information. Just prior to that date, British Columbia and Alberta each enacted a *Personal Information Protection Act* while, in 1993, Quebec had enacted the *Loi sur la protection des renseignements personnels dans le secteur privée*.[2]

As of the time of writing, no announcement had been made as to whether the personal information protection statutes of Alberta and British Columbia were to be designated "substantially similar" to PIPEDA.[3] Quebec's legislation has been designated "substantially similar" to PIPEDA.

Federal

PIPEDA is a statute with five parts. Part One deals with the protection of personal information in the private sector[4] and is, in turn, divided into five divisions. Division 1 outlines the rules for the collection, use, and disclosure of personal information in the course of commercial activities; Division 2 sets out the remedies; Division 3 provides for privacy audits; Division 4 deals with general matters; and Division 5 sets out the transitional provisions.

When looking to develop national rules to protect personal information, the Canadian government turned to the Canadian Standards Association ("CSA") Model Code,[5] a voluntary industry-developed code. The CSA Model Code was designed to provide businesses with some minimal guidelines concerning the protection of personal information in their care and control. The government adopted the CSA Model Code without any changes or amendments as a schedule (the "Schedule") to its legislation and then modified the Schedule by including sections to deal with new issues such as the application of the law, or by including sections that override specific provisions. The language of the CSA Model Code, as a voluntary industry standard, is inherently vague. While some provisions, such as the exceptions for obtaining consent, have been clarified, other concepts, such as the definition of "sensitive" information, have been left for the courts to determine. It is also difficult to assess the risks of non-compliance. The result is a statute that is unusually difficult to work with.

PIPEDA applies to federally regulated industries such as banks, railways, inter-provincial trucking companies, airlines and telecommunication companies (regardless of location), to all businesses in the Yukon, Northwest Territories and Nunavut, and to personal information disclosed across borders for commercial purposes.

To determine the substantive portions of PIPEDA, one must start with the Schedule and then turn to Part One of the legislation. The Schedule, and hence PIPEDA, has ten guiding privacy protection principles. These principles focus on the core elements of notice, consent, security, and access.

Principle 1: Accountability

All organizations in Canada are responsible for protecting the personal information under their control. It is the organization that is held accountable to ensure the protection of the personal information and is specifically responsible to protect personal information that has been transferred to a third party.

To comply with this principle, organizations are, at a minimum, required to implement policies and train staff that give effect to PIPEDA as well as appoint a designated person – a privacy compliance officer – to oversee compliance. Most organizations should consider taking the following steps:

- Ensure that the privacy compliance officer has senior volunteer and management support, and the authority to intervene on all privacy issues within the organization's operations.
- Publicize the name or title of the privacy compliance officer internally and externally.
- Analyze all personal information handling practices, including ongoing activities and new initiatives.[6]
- Develop and implement policies and procedures to protect personal information.[7]
- Include a privacy protection clause in contracts to guarantee that the third party (the party that the organization is contracting with) provides the same level of protection as the organization.
- Inform and train staff and applicable volunteers (including those who are regionally located) on privacy policies and procedures.
- Provide information (through brochures, Web sites, etc.)[8] explaining these policies and procedures to stakeholders.

Principle 2: Identifying the Purposes

Section 5(3) of PIPEDA provides that "an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." This section provides the limits that may be used by an organization to justify collection, use, or disclosure and bases it on the objective standard of the "reasonable person." Obtaining the consent of the individual for the collection of personal information outside the limit of "what a reasonable person would consider appropriate in the circumstances" would likely result in a failure to comply with PIPEDA.

Therefore, every organization must determine the purposes for which it collects personal information. This is usually done by conducting an audit of the organization. Once identified, those purposes must be communicated to the individual at or before the time that the personal information is collected. Finally, once collected, the personal information cannot be used for a new or further purpose without the (additional or new) consent of the individual. It is, therefore, critical to determine all possible purposes and to define them sufficiently in order to avoid having to return to the individual for additional consent.

Therefore, an organization should consider taking the following steps to ensure compliance with this principle:

- Review personal information holdings to ensure they are all required for a specific purpose.
- Notify the individual, either orally or in writing, of these purposes.
- Record all identified purposes and obtain consents for easy reference in case an individual requests this information.

- Ensure that these purposes are limited to what a reasonable person would expect under the circumstances.

Principle 3: Consent

This principle is generally regarded as the core of PIPEDA. Generally, personal information cannot be collected, used, or disclosed without the consent of the individual, unless there is a specific exemption provided for in PIPEDA. Further, an organization may not, as a condition of the supply of a product or service, require consent beyond what is required for the legitimate fulfillment of the transaction.

The difficulty with this principle is determining the degree of consent required. PIPEDA has a particular focus on informed consent as to the collection, use, and disclosure of the individual's personal information. Consent may therefore be "express" or "implied," or "opt-in" or "opt-out," depending upon the degree of consent required. In turn, that degree of consent depends upon the sensitivity of the information. For example, implied consent, such as when an individual provides personal information when filling out an application form, may suffice. Alternatively, express consent, such as signed consent, may be required to disclose information to third parties.

As an example of ensuring compliance on an "implied" consent basis, the members of the Canadian Direct Marketing Association follow the guidelines established by that organization. The guideline states that to assert "implied" consent, organizations would need to:

- develop a meaningful statement of the implied consent option (opt-out);
- provide the statement in a prominent manner with as specific information as possible about the nature of the proposed uses of the information;
- ensure the option is easy to execute, preferably with a check-box, postage-paid reply card or a 1-800 number;
- provide the option before any information is used or disclosed; and
- provide the option on a regular basis, such as every three years at a minimum.

The former federal Privacy Commissioner was not a fan of opt-out consent as shown in his findings regarding Air Canada's Aeroplan Frequent Flyer Program, released March 20, 2002:

> "I should begin by making it clear that, like most other privacy advocates, I have a very low opinion of opt-out consent, which I consider to be a weak form of consent reflecting at best a mere token observance of what is perhaps the most fundamental principle of privacy protection. Opt-out consent is in effect the presumption of consent – the individual is presumed to give consent unless he or she takes action to negate it. I share the view that such presumption tends to put the responsibility on the wrong party. I am also of the view that inviting people to

> opt-in to a thing, as opposed to putting them into the position of having to opt-out of it or suffer the consequences, is simply a matter of basic human decency.
>
> Accordingly, while acknowledging that the *Act* does provide for the use of the opt-out consent in some circumstances, I intend, in this and all future deliberations on matters of consent, to ensure that such circumstances remain limited, with due regard both of the sensitivity of the information at issue and to the reasonable expectations of the individual. In other words, in interpreting Principle 4.3.7, I intend always to give full force to other relevant provisions of the *Act*, notably 4.3.4, 4.3.5 and 4.3.6 and section 5(3)."

As consent under PIPEDA is linked to the "sensitivity" of the information collected, used, or disclosed and the concept of "sensitivity" is subjective, this principle has led to much discussion.

There are specific exemptions in PIPEDA to consent. Consent is not needed for *collecting* personal information if:

- it is clearly in the interests of the individual;
- it is to be used for the investigation of a breach of agreement or a contravention of a federal or provincial law, and consent would compromise the collection;
- it is to be used solely for journalistic, artistic, or literary purposes; and
- it is publicly available information as specified in the regulations.

Consent is not needed for the *use* of personal information if:

- it is to be used to investigate the contravention of the laws of Canada, a province, or a foreign jurisdiction;
- there are life, health, or security consequences;
- it is to be used for statistical or scholarly research; or
- it is publicly available or attached under exemptions under collection – in the interests of the individual or investigation of a search of agreement or contravention of a federal or provincial law.

Consent is not needed for the *disclosure* of personal information if it is:

- to a lawyer representing the organization;
- for debts owed to the organization;
- for compliance with a court or similar order;
- disclosure to government for identified purposes;
- for the investigation of a breach of agreement;
- in life, health, or personal security emergencies;
- for statistical or scholarly research;
- for historical or archival records;

- 100 years after the creation of the record, or 20 years after the death of the individual; or
- publicly available information.

PIPEDA also speaks of the withdrawal of consent. Consent may be withdrawn at any time, subject to legal or contractual restrictions and reasonable notice.

As an example, in Case Summary #249, a customer of the bank received a notice that the language of the consent clause was being changed. She called the toll-free number several times but was unable to get through. When the call was connected, she was not able to speak with a representative; instead she received another recorded message suggesting she write the bank. The complaint was found to be well-founded.

The prudent course has been, when possible, to obtain written consent. However, additional steps to ensure compliance include the following:

- Communicate clearly in understandable terms.
- Ensure that staff collecting personal information are able to answer questions about the purposes of the collection.
- Obtain appropriate consent from the individual whose personal information is collected, used, or disclosed.
- Record the consent received (e.g., note to file, copy of e-mail, copy of check-off box).
- Never obtain consent by deceptive means.
- Do not make consent a condition for supplying a product or a service, unless the information requested is required to fulfill an explicitly specified and legitimate purposes.
- Be able to explain the implications of withdrawing consent.

In Case Summary #271, an individual continued to receive unwanted credit card offers from a bank despite asking the bank to stop sending such solicitation documents. The bank tried to take the individual's name off but the name was not taken off because the individual's given name was not entered correctly in the data bank. The complaint was found to be well founded even though the bank had, during its investigation, successfully removed the name.

Principle 4: Limiting Collection

This principle provides that the collection of personal information must be limited to that which is necessary for the purposes identified by the organization and that these purposes must be reasonably specific.

Further, the information must be collected by fair and lawful means.

To ensure compliance the following steps should be considered:

- Limit the amount and type of the information gathered to what is reasonably necessary for the identified purposes.
- Identify the kind of personal information collected in your information handling policies and practices.
- Ensure that staff are able to explain why the information is needed.

Principle 5: Limiting Use, Disclosure, and Retention

Organizations are not permitted under PIPEDA to use or disclose personal information for purposes other than those for which it was collected, unless the individual consents or as required by law. Further, organizations must only retain the personal information for as long as it is necessary for the fulfillment of those purposes. Therefore this principle requires organizations to develop guidelines that include maximum and minimum retention periods to ensure that personal information is retained only for so long as is necessary.

In Case Summary #252, an individual complained that a bank was not properly retaining mortgage renewal acknowledgment letters for its clients. The bank destroyed the information two years after each mortgage discharge (if registered) and six years after discharge (if not registered). The complaint was found to be not well founded.

The following steps could be considered to ensure compliance with this principle:

- Document any new purpose for the use of personal information.
- Dispose of information that does not have a specific purpose or that no longer fulfills its intended purpose.
- Dispose of personal information in a way that prevents improper access, such as shredding paper files or deleting electronic records.
- Institute maximum and minimum retention periods that take into account any legal requirements or restrictions and redress mechanisms.
- As it can be reasonably expected that individuals will provide updated information in certain circumstances (e.g., change of address for a magazine subscription), establish policies setting out the types of information that need to be updated.

Principle 6: Accuracy

Organizations must ensure that the personal information under its control is as "accurate, complete and up-to-date" as is necessary for the purposes for which it is to be used. This principle is vaguely worded, suggesting that compliance depends upon the use of the information and the interests of the individual.

To ensure the accuracy of the personal information, the following steps should be considered:

- Determine and keep personal information as accurate, complete, and up-to-date as necessary, taking into account its use and the interests of the individual.
- Update personal information only when necessary to fulfill the specified purposes.
- Keep frequently used information accurate and up-to-date, subject to any established limitations.

Principle 7: Safeguards

This principle provides that an organization must protect the personal information under its control by appropriate security safeguards. The purpose of the safeguards is not just to protect against theft, but also to protect against unauthorized access, disclosure, copying, or use.

The appropriateness of the safeguards depends upon such things as the sensitivity and amount of the information, the extent of distribution, the format of the information, and the type of storage. However, the methods of protection must include *physical measures*, such as locked filing cabinets or restricted access; *organizational measures*, such as security clearances, staff training, confidentiality agreements, and access on a "need-to-know" basis; and *technological measures* such as passwords, encryptions, anonymizing software, and firewalls. Conducting audits on a regular basis to ensure compliance is recommended.

A reminder on "appropriate security": In September 2003, the story was reported that "smash and grab" thieves stole a computer containing tax information on 120,000 Canadians. The computer was portable and not locked. The data was not encrypted. There was (in retrospect) inadequate protection of personal information. This incident demonstrates that a significant threat to the protection of personal information may actually be the loss or disposal of the computer hardware.

The following steps should be considered as ways to safeguard personal information:

- Develop and implement a security policy to protect personal information.
- Make staff and volunteers aware of the importance of maintaining the security and confidentiality of personal information.
- Ensure staff and volunteer awareness by holding regular training on security safeguards.
- Review and update security measures regularly.
- Use appropriate security safeguards to provide necessary protection in the three areas of physical measures, technological tools, and organizational controls, having regard to the following factors:
  - sensitivity of the information,
  - amount of information,

- extent of distribution,
- format of the information (electronic, paper, etc.), and
- type of storage.

Principle 8: Openness

An organization must have readily available specific information about its policies and practices relating to the management of personal information. This principle requires the development of privacy statements for Web sites, personnel resource, or other organizational materials.

The information that should be made available includes:

- the name or title, and the address, of the person at the organization accountable for personal information;
- information on how to gain access to personal information held by the organization;
- a description of the type of personal information held by the organization, including a general account of its use;
- a copy of any brochure that explains the organization's policies, standards, or codes; and
- a summary of what personal information, if any, is made available to third parties.

Principle 9: Individual Access

Upon request, an organization must inform individuals of the existence, use, and disclosure of their personal information and individuals must also be allowed access to that information. In addition to all staff being aware of the organization's privacy compliance officer, the privacy compliance officer should also keep records of complaints and inquiries.

An individual is allowed to challenge the accuracy and completeness of the information and have it amended as appropriate. Accordingly, an individual has a right to access. This right to access is, however, limited by the provisions of sections 8 and 9 of the PIPEDA, which set the terms for requesting access and prescribe when access is prohibited[9] or may even be refused by the organization.[10] There are also statutory exceptions to provide access for such matters as documents prepared for litigation and documents that contain proprietary business information, such as credit scores, which can be "reverse engineered" to reveal proprietary information. Under PIPEDA, disclosure includes an account of the use that has been made of the information and any third parties to whom the information has been disclosed.

The organization must respond to the request no later than 30 days after receipt of the request, unless the permitted grounds for an extension of time apply. As an example,[11] in Case Summary #272, an individual alleged in furtherance to his credit card application that the bank did not respond to his request for

personal information. Eventually the bank sent a written reply more than 38 days after receipt of the request. The complaint was found to be well founded.

In another example, in Case Summary #253, an individual complained the bank did not answer a request for personal information regarding the individual's application for a credit card. It was only after five months and after the Office of the Commissioner intervened that the bank answered the request (in part). The complaint was found to be well founded.

Section 8(4) of PIPEDA permits the time limit to be extended for a maximum of 30 additional days if:

- responding to the request within the original 30 days would unreasonably interfere with activities of the organization;
- additional time is necessary to conduct consultations; or
- additional time is necessary to convert personal information to an alternate format.

An organization is prohibited from charging the individual making the request the full cost of the disclosure. Responses to requests must be provided at minimal or no cost[12] and the individual may be required to pay only if the individual is notified in advance of the approximate cost and agrees to pay. An organization, according to the Privacy Commissioner, should only charge processing fees when the request is "exceptional" and then only at "minimal" cost.

As an example, in Case Summary #247, a bank wanted to charge an individual between $500 and $800 for access to information about an old account that had been closed for a long time. After it was pointed out that personal information is to be provided at minimal or no cost, the fee was reduced to $75.

In Case Summary #283, a bank charged $25.00 to respond to a personal information request. The complaint was found to be well founded. After investigation of the complaint, the bank informed the Privacy Commissioner that its policy had been changed and that the fee for such a service was now $5.00. Despite the reduction to a "nominal fee," the Assistant Privacy Commissioner recommended that the bank cease charging even the $5.00 fee.

Steps to consider taking in order to comply with this principle include:

- Provide any help to the individual in preparing a request for access to personal information.
- Ensure that the individual supplies enough information to enable the organization to account for the existence, use, and disclosure of personal information.
- Respond to the request as quickly as possible and no later than 30 days after receipt of the request.
- If the time is extended, notify the individual making the request of the extension within 30 days of receiving the request, including his or her right to complain to the Privacy Commissioner.

- Give access at minimal or no cost to the individual.
- Notify the individual of the approximate costs before processing the request.
- Make sure the requested information is understandable (e.g., explain acronyms, abbreviations, and codes).
- Send any information that has been amended, where appropriate, to any third parties that have access to the information.
- Inform the individual in writing when refusing to give access, setting out the reasons and any recourse available.

Finally, disclosure can be an expensive process, especially if the files containing such information have not been properly structured in advance to record and summarize such information as use occurs. It is therefore recommended that each file entry be made as if in anticipation of a request being made.

Principle 10: Challenging Compliance

An organization has an obligation to be ready to respond to challenges to its compliance with PIPEDA. As these challenges are to be channeled through the organization's privacy compliance officer, there should be policies and procedures for dealing with complaints and challenges.

To comply with this principle, organizations should consider the following steps:

- Record the date a complaint is received and the nature of the complaint (e.g., delays in responding to a request; incomplete or inaccurate responses; or improper collection, use, disclosure, or retention).
- Acknowledge receipt of the complaint promptly.
- Contact the individual to clarify the complaint, if necessary.
- Assign the investigation to a person with the skills necessary to conduct it fairly and impartially.
- Give the investigator access to all relevant records and to staff or others who handled the personal information or access request.
- Notify individuals of the outcome of the investigations clearly and promptly, and inform them of any relevant steps taken.
- Correct any inaccurate personal information or modify policies and procedures based on the outcome of the complaint.

For example, in Case Summary #260, an individual complained that a company from which she had purchased a product sold her name and address to third parties without her consent. The company was very proactive in resolving the complaint, for which it was commended. As a result, the finding of the privacy commissioner was that the complaint was resolved.

Application and Compliance

PIPEDA does not apply to the federal government, to information collected for domestic purposes or for journalistic, artistic, or literary purposes, or to information that is publicly available (to be specified in regulation).

For organizations to which PIPEDA applies, application of the law depends in large measure upon the definitions of "personal information" and "commercial activities." The definition of "personal information" is "information about an identifiable individual but does not include the (business) name, title or business address or telephone number of an employee or organization." This includes any personal information in any form, including digital or paper format. For example, the following would be considered personal information:

- age identification numbers, name, blood type, and gender;
- credit and loan records, wealth, and income memberships,
- existence of a dispute between a consumer and an organization (unless in the public domain); and
- intentions to acquire goods or services, opinions, and evaluations.

Note the exceptions to the definition for the name, business title, business address, business telephone of an employee, or what is described as "business card" information. Note, too, that the individual's e-mail address is not on the list even though it regularly appears on a person's business card. Giving someone your business card, however, would likely constitute implied consent to use the e-mail address.

For example, in Case Summary #277, eleven members of a loyalty program complained that the company that ran the program failed to safeguard their personal information – namely their e-mail addresses – and as a result had disclosed it to other members. The complaint was found to be well founded.

The legislation also protects personal information that is considered of a sensitive nature. This may include health or medical history, racial or ethnic origin, political opinions, religious beliefs, trade union membership, and sexual orientation.

The definition of "personal information" is key because if the information collected, used, or disclosed is not personal information as defined, then PIPEDA does not apply.

There have been some decisions in this area. In Case Summary #240, during an investigation, it was determined that the individual's information related solely to the complainant's business account at a bank. The business was incorporated, and the individual was the sole director. The Commissioner stopped the investigation on the grounds that the information was not "personal information" within the meaning of PIPEDA.

In Case Summary #236, cheques drawn on a trust account were found to contain the personal information of the trust beneficiaries even though they were not the account holders. The fact that they had beneficial rights to the money was sufficient to make the information "personal."

Likewise, the definition of "commercial activity" is key. This issue is central because the application of PIPEDA to the private sector (which includes charities) is limited to the collection, use, and disclosure of personal information in the course of "commercial activities."

"Commercial activity" is defined as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists." It is a broad definition including the traditional and less traditional concepts of an exchange of consideration. It catches more than the usual purchase or sale of goods and services – as any exchange of consideration, with consideration including more than money, will be caught. Note further the emphasis in the definition of the phrase "of a commercial character." In other words, any act that "walks like, talks like, or looks like" a commercial transaction will likely be considered "commercial activity."

The general view is that "commercial activity" likely also includes a single isolated act of commercial activity by "non-commercial" organizations.[13] Further, organizations, such as charities and not-for-profit organizations, that engage in commercial activities ancillary to their primary purposes are likely subject to PIPEDA to the extent that commercial activity involves the collection, use, or disclosure of personal information (leaving aside the constitutional question).

Quebec

Quebec follows the French civil code model and is often influenced by developments in France and in Europe. Privacy is no exception. Quebec has had private sector privacy legislation since 1994.

To expand upon the information privacy rights provisions (Articles 35–41) of the *Code civil*, in 1993 Quebec introduced the *Loi sur la protection des renseignements personnels dans le secteur privée.*[14] This legislation sets the standards with respect to the collection and use of personal information, including having a defined purpose or object, collecting only the necessary information, informing the person from whom the file is established, and obtaining consent for transferring such information to a third party.

Article 35 of the *Code civil du Québec*[15] states:

> Art. 35 Toute personne a droit au respect de sa réputuation et de sa vie privée.
>
> Nulle attente ne peut être portée a la vie privée d'une personne sans que celle-ci uses heritiers y consentent ou sans que la loi l'autorisé.

Article 36 goes on to illustrate items that might be considered the invasion of the privacy of a person. These include entering or taking anything from a person's dwelling, intentionally intercepting or using their person's private communication; approaching or using the person's image or voice when the person is in private premises; keeping the person's private life under observation by any means; using the person's name, image, likeness, or voice for a purpose other than providing legitimate information to the public; or using the person's correspondence, manuscripts, or other personal documents. Further, pursuant to section 70, every personal information agent (defined as a person who, on a commercial basis, personally or through a representative, establishes files on a person) must register with the *Commission d'access à l'information du Québec*. The Commission deals with the public sector under separate legislation.

In the event of a dispute, a person may file an application with the *Commission d'acces à l'information du Québec*. Appeals from the decisions of the Commission are to a judge of the Court of Quebec.

Since the law governing private sector collection of personal information came into force on January 1, 1994, the Commission and the courts have rendered over 1,200 decisions on privacy matters. There is also a quarterly bulletin and an annual review of the decisions concerning privacy.

It is generally considered that the Quebec law is working well. It was, therefore, a bit of a surprise when, on December 17, 2003, the Quebec Attorney General was asked by the National Assembly to submit the question of PIPEDA's constitutionality to the Quebec Court of Appeal. The reason given was that PIPEDA oversteps constitutional powers by granting to the Governor in Council the power to determine if a provincial law is "substantially similar" and therefore whether it can continue to operate. Although the previous Parti Québécois government adamantly opposed PIPEDA as a statute that eroded Quebec powers, it was not totally expected that the Liberal government would take the same view and then wait until December 2003 to launch a challenge.

This constitutional issue will probably be resolved in the Supreme Court of Canada (with the other provinces potentially joining forces), leaving that Court to determine whether the federal government has the power to declare a provincial law operating provincially as "inadequate" and, therefore, replaceable by a federal law.

Alberta

Alberta's *Personal Information Protection Act, 2003*[16] (Alberta PIPA, formerly Bill 44) was introduced into the legislation on May 14, 2003, received Royal Assent on December 4, 2003, and came into force as of January 1, 2004. Alberta has also passed Regulation 366/2003 relating to this statute.

The Alberta PIPA operates[17] from the same basic premise as PIPEDA, with the similar purpose of governing the means by which private sector organizations handle personal information in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use, or disclose personal information for purposes that are reasonable. As a statute it has a particular focus on "reasonableness" and includes a provision as to the "standard as to what is reasonable."[18]

The Alberta PIPA is based on "fair information practices" similar to PIPEDA, such as:

- being accountable;
- identifying the purpose for collecting information;
- obtaining consent;
- limiting collection, use, disclosure, and retention;
- being accurate;
- using appropriate safeguards;
- being open about management practices; and
- providing access to individuals and allow challenges to compliance.

The Alberta PIPA applies to "every organization and in respect to all personal information."[19]

Some examples of the organizations to which the Alberta PIPA applies include:

- nonprofit organizations,
- trade unions,
- private schools,
- partnerships,
- corporations,
- unincorporated associations,
- professional regulatory associations,
- any individual acting in a commercial capacity (but not in a personal or domestic capacity), and
- any individual acting on behalf of a corporation, unincorporated association, trade union, or partnership.

The Alberta PIPA does not apply to the collection, use, or disclosure of personal information if:

- it is for domestic, historic, or literary purposes;
- it is "business contact information";
- it relates to personal information in the custody of a "public body";
- it is health information under the *Health Information Act*;
- it is by an officer of the Legislature;

- the individual has been dead for at least 20 years;
- it is contained in a record that has been in existence for at least 100 years;
- it is contained in a record transferred to an archival institution;
- it is contained in a court file;
- it is contained in a record created by a member of the Legislative Assembly or appointed member of a public body;
- it is by a "bona fide" candidate for public office; or
- it is contained in a personal note or draft decision by or for a person in a judicial or quasi-judicial capacity.

Under the Alberta PIPA, "personal information" is everything there is to know about an individual. It is defined as "information about an identifiable individual."[20] As with BC PIPA, the Alberta PIPA includes other definitions relating to personal information. "Business contact information" means an individual's name, position name or title, business telephone number, business address, business e-mail, business fax number, and other similar business information.

Significantly, the Alberta PIPA allows for grandfathering of personal information collected and stored prior to January 1, 2004. This information is "deemed to have been collected with consent" and may be used for the purposes originally intended. If an organization had under its control personal information about an individual that was acquired prior to January 1, 2004, that information, for the purposes of the statute, is deemed to have been collected pursuant to the consent given by the individual and may be used and disclosed by the organization for the purposes for which the information was collected. However, as of January 1, 2004, that information is to be treated in the same manner as information collected under the statute.[21]

The Alberta PIPA also significantly permits the collection, use, or disclosure of personal information for particular purposes without express consent if:

- the organization provides understandable notice of the organization's purposes with respect to the individual's information;
- the organization gives reasonable opportunity for the individual to decline or object within a reasonable time to having his or her personal information collected, used, or disclosed;
- the individual does not decline within a reasonable time; and
- the collection, use, or disclosure is reasonable having regard to the "sensitivity" of the information "in the circumstances."[22]

Further, even aside from grandfathering, the Alberta PIPA "deems" consent to the collection, use, and disclosure of personal information if the individual voluntarily provides the information and it is reasonable that a person would voluntarily provide that information.[23] For example, if an individual asks to receive a newsletter, it is inferred that he or she has consented to the organiza-

tion keeping the information on file and accessing that information to send the newsletter.

Consent may be withdrawn or varied.[24]

Similar to PIPEDA, the Alberta PIPA states that "commercial activity" includes "the selling, bartering and leasing of membership lists or of donor or other fund raising lists."

The Alberta Information Management, Access and Privacy Division has prepared a series of Frequently Asked Questions and Information Sheets available online. This material provides some guidance in determining whether a transaction is a "commercial activity" for the purposes of the Alberta PIPA. Some considerations mentioned include:

- Does the activity involve consideration by one party (rather than consideration for both parties)?
- Is the activity one that tends to be provided only by the government or nonprofit sector (rather than by private sector businesses)?
- Is the activity financially supported by the activities of the organization or operated on a cost recovery basis (rather than intended to make a profit to be used to support other activities)?
- Is the primary purpose of the activity to provide a public benefit (rather than benefit individual participants or clients)?
- Is the activity conducted for the purpose of fundraising for charitable purposes (rather than to raise funds for regular operations or non-charitable purposes)?

This material also provides examples of commercial activities, such as the sale of merchandise within the province, the sale of collected personal information (e.g., from conference registrants), the provision of counseling for a fee, and other activities where the intent is to make a profit (e.g., courses).

Under the Alberta PIPA, the rules governing disclosure have been expanded. The Alberta PIPA expressly allows the disclosure of personal information without consent for the purpose of mergers and acquisitions provided that the information is used for that sole purpose and on the condition that if the merger and acquisition does not proceed, the potential buyer will destroy or return the personal information.

Under the Alberta PIPA, the organization's privacy compliance officer is responsible for assisting individuals with concerns or requests in relation to the access, collection, use, or disclosure of their own personal information, including personal employee information.

After making a request, the individual can request a correction of the personal information held by the organization. The organization must respond to the request within 45 days. If not satisfied with the response, the individual may

request a review of the decision by the Commissioner. The Commission will assign an officer to facilitate resolution between the parties. If that fails, the Commissioner may decide to authorize a review. The Commissioner can either uphold or over-rule the organization's decision.

Generally speaking, before requesting a review of an organization's actions, the individual is encouraged to exhaust all means of resolving his or her concerns with the organization. A copy of the request for a review will be sent to the organization. If mediation fails, the Commissioner will decide whether to conduct an inquiry. An inquiry is the final conclusion to a review or investigation. This is a formal proceeding that allows the Commissioner to hear everyone involved and to make a decision. The inquiry may be in writing or orally. The Commissioner's decision is final.

Interestingly, the Office of the Information and Privacy Commissioner has issued "Information and Guidelines for an Advance Ruling Under Alberta's *Personal Information Protection Act*." These guidelines describe an advance ruling (a request that is not a legal precedent and only applies to the requesting organization) and sets out guidelines for making and publishing advance rulings.

Finally, it is noted that the Alberta PIPA does not apply to health information, as defined in Alberta's *Health Information Act* regulated by Alberta Health (<www.health.gov.ab.ca>) or organizations covered by the *Freedom of Information and Protection of Privacy Act*, which came into to force April 25, 2001 but does cover professional regulatory organizations including health professionals.[25]

British Columbia

On April 30, 2003, the Minister of Management Services for British Columbia introduced (formerly Bill 38) its own *Personal Information Protection Act* (BC PIPA) to protect personal information held by the private sector. It came into force on January 1, 2004.[26]

The BC PIPA applies to more than 350,000 private sector organizations in British Columbia, including businesses, charities, associations and labour organizations, and sets out the rules on how those organizations may collect, use, and disclose personal information – customers' and employees' "personal information."

It applies to all provincially regulated private sector "organizations." It covers all corporations, partnerships, sole proprietorships, trusts, trade unions, not-for-profit organizations, unincorporated associations, and individuals acting as agents or contractors. The BC PIPA qualifies the term "organization" by stating that some entities are not organizations (and so are not covered). The following entities are deemed not to be organizations for the purpose of the BC PIPA:

- an individual acting in a personal or domestic capacity or acting as an employee;
- a public body as defined in the *Freedom of Information and Protection of Privacy Act*;
- the Provincial Court, the Supreme Court, or Court of Appeal;
- the Nisga's Government, as defined in the Nisga's Final Agreement; or
- a private trust for the benefit of one or more designated individuals who are friends or members of the family of the settler.

The BC PIPA also applies to nonprofit organizations, including trade unions, charities, foundations, trusts, clubs, churches, and amateur sports organizations. Not-for-profit organizations in British Columbia (regardless of the location of the organization's headquarters) are in the same position as for-profit organizations and subject to the legislation in respect of all their activities, not simply to any potential "commercial activity."

The BC PIPA applies unless an exemption set out in section 3(2) applies. Those exemptions include any "public body" covered by British Columbia's *Freedom of Information and Protection of Privacy Act* or to personal information to which that *Act* applies, the collection, use, or disclosure of personal information for domestic, artistic, literary, or journalistic purposes or personal information in documents related to the judicial system, or information collected on or before January 1, 2004.

Therefore, the BC PIPA differs fundamentally from PIPEDA in that it applies to the entire private sector and applies to the collection, use, and disclosure of personal information in the course of both commercial and non-commercial activities (such as fundraising or the provision of services for no consideration). In effect, the BC PIPA applies (subject to the exceptions) to all organizations operating in the province. The fact that an organization may be headquartered or incorporated elsewhere does not preclude the application of the BC PIPA. Accordingly, the starting point of an organization that collects, uses, and discloses personal information in the province of British Columbia should be the BC PIPA.

However, it is similar to PIPEDA in that the BC PIPA imposes obligations upon organizations in respect to the collection, use, and disclosure of personal information, and, although not specifically incorporated, the CSA Model Code is also at the core of the legislation. Although quite detailed,[27] in summary, the BC PIPA prohibits the collection, use, and disclosure of personal information without notice of the purposes required and the consent of the individual.

The BC PIPA operates from the same basic premise as PIPEDA, namely that "personal information" is everything there is to know about an individual. Personal information is defined as "information about an identifiable individual including employee personal information but does not include contact

information on work product information." In turn, "contact information" is defined to mean "information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business e-mail or business tax number of the individual." "Work product information" means information prepared or collected by an individual or group of individuals as a part of the individual's or group's responsibilities or activities related to the individual's or group's employment or business but does not include personal information about an individual who did not prepare or collect the personal information."

Personal information can therefore only be collected for reasonable purposes, and only the amount and type of information reasonably needed to carry out the purposes for collecting it can be collected. Notice about why the personal information is being collected before, or at the time, of collection is usually needed.

The BC PIPA, unlike PIPEDA, also directly addresses the issue of implied consent. The BC PIPA considers consent ("deemed consent") to be given when an individual, knowing of the purpose of collection of his or her information, gives the information to the organization. An individual is, therefore, deemed to consent to a purpose that at the time "would be considered to be obvious to a reasonable person" and if the individual voluntarily provides the personal information for that purpose. An individual is also deemed to consent to the collection, use, and disclosure of personal information for the purpose of enrolment for coverage under an insurance, pension, benefit, or similar plan if the individual is a beneficiary or has an interest as an insured under the plan.[28]

Express guidelines for "opt-out" consent are also provided. An organization may collect, use, or disclose personal information for specified purposes if these four conditions are met:

- the individual is given understandable notice of the organization's purposes with respect to his or her information;
- the individual is given reasonable opportunity to decline within a reasonable time to have his or her information collected, used, or disclosed for those purposes;
- the individual did not decline within that reasonable time; and
- the collection, use, or disclosure must be reasonable having regard to the "sensitivity" of the information "in the circumstances."[29]

Consent may also be withdrawn on reasonable notice.[30]

An organization may collect personal information without consent in certain circumstances, such as:

- The collection is clearly in the individual's interests and consent cannot be obtained in a timely way.

- The collection is necessary for the medical treatment of the individual and the individual is unable to give consent.
- It is reasonable to expect that consent would compromise the availability or accuracy of the information where the collection is reasonable for an investigation as proceeding.
- It is collected by observation under certain conditions.
- It is necessary to determine the individual's suitability to receive an honour or award.
- The organization is a credit reporting agency.
- It is authorized by law.
- It is necessary to facilitate the collection or payment of a debt.

An organization may also use personal information without consent in certain circumstances. These circumstances are similar to those exceptions set out for the collection of personal information without consent.

Similarly, the same type of exceptions apply for the disclosure of personal information without consent. In addition, disclosure without consent is permitted where:

- it is for the purpose of complying with an order or warrant;
- it is to a public body or law enforcement agency in Canada;
- there are reasonable grounds to believe that "compelling circumstances" exist that affect the health or safety of an individual;
- it is for the purpose of contacting next of kin or a friend of an injured, ill, or deceased person;
- it is to a lawyer who is representing the organization; or
- it is to an archival institution if the collection is reasonable for research or archival purposes.

Further, an organization may disclose to another organization without consent if the individual consents to the collection of the personal information by the organization and the personal information is disclosed solely for the purposes for which the information was previously collected and to assist the other organization to carry out work on behalf of the first organization.[31]

The BC PIPA further expressly provides disclosure rules for outsourcing and due diligence investigations and transfer of information on closing for a "business transaction." A business transaction is defined to include "a purchase, sale, lease, merger or amalgamation or any other type of acquisition, disposal or financing of an organization or portion of an organization or any of its business or assets." When buying or selling a business, the information may be collected, used, and disclosed without consent when those involved agree to do so only for the transaction and when they need the information to decide whether to buy or sell. Once the transaction is completed, the organiza-

tion receiving the personal information may continue to use and disclose it, but the information can only be used and disclosed for the purpose for which it was originally collected. Further, the information must relate solely to the carrying on of the business. If the transaction does not proceed, the organization that received the personal information must destroy or return it.[32]

Each organization is still required to decide whether getting express written consent is desirable. When deciding on the type of consent, what is reasonable for the individual, the circumstances of collection, the proposed uses or disclosures of the information, the sensitivity of the information, and whether the organization may need to prove that the individual consented, are factors to consider.

Organizations must also permit individuals to access and correct their personal information on request and adopt reasonable procedures to restrict access to personal information and provide security to prevent unauthorized disclosure. Individuals have a right to be given access to their own personal information, to know how their information is being or has been used, and know to whom and in what situations the information has been disclosed. Requests may be made to which the organization must respond within 30 days (or an extended time if the provisions of section 31 are met). If access is refused, the organization must advise the individual of the reasons, the contact information of the privacy compliance officer, and that a review may be requested within 30 days of the notification.[33] Organizations may charge a "minimal" fee for access, but cannot charge a fee to their employees for giving access to employee personal information.[34]

The BC PIPA has similar requirements to PIPEDA regarding the care of personal information. Such information must be protected by "making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks."[35]

Under the BC PIPEDA, personal information must be retained for at least one year where that information has been used to make a decision that directly affects the individual. Otherwise personal information must be destroyed or the organization must remove the means by which the personal information can be associated with particular individuals "as soon as it is reasonable" to assume that the purpose is no longer being served and retention is no longer necessary for "legal or business purposes."[36]

Further, the BC PIPA has particular rules for "employee personal information" and considers employees to include volunteers. An employer is also allowed to collect, use, and disclose "employee personal information" without consent if the individual is given advance notification by the employer and the sole purpose is establishing, managing, or terminating an employment relationship.

The BC PIPA also allows the collection, use, and disclosure of personal information that is "work product information" or information collected by an individual or group during activities relating to employment or business.

Finally, the BC PIPA requires organizations to adopt and implement a privacy policy and to appoint an individual in the organization to administer the policy while relying heavily upon the "reasonable person test" for deciding whether an organization has carried out its BC PIPA responsibilities.

Ontario

Presently, Ontario does not have privacy legislation that governs the private sector as the latest attempt was delayed by an election call. A prior attempt, Bill 159, introduced December 7, 2000, had also died on the order pages. That attempt resulted in the draft *Privacy of Personal Information Act, 2002* ("PPIA") which, in an attempt to be declared "substantially similar" to PIPEDA, required 120 pages to incorporate the principles of the CSA Model Code into legislation.

PPIA departed significantly from PIPEDA. First, it attempted to apply to both general and health-related personal information. It contained much of the same framework as the prior legislative attempt (Bill 159), but combining general and health-related personal information caused difficulties. Second, PPIA had an expanded scope. It included within its mandate charities, other not-for-profit organizations, including hospitals and educational institutions, as well as rules for protecting personal information of employees of every business or organization in Ontario. Third, on the fundraising side, objections were raised regarding the provisions that donors or other individuals would have to opt-in (positively assert consent) before use could be made of their personal information, the provisions that restricted the use of public information to generate contact lists and data bases on next-of-kin, and the lack of a grandfathering provision dealing with the treatment of existing data bases of personal information. This legislation would have dramatically extended privacy protection beyond PIPEDA and, likely, charitable and not-for-profit organizations breathed a sign of relief with that election call.

There have been legislative developments in the health sector. In December 2003, Ontario introduced Bill 31 (first reading December 17, 2003; second reading March 2004). The *Health Information Protection Act, 2004* came into force on November 1, 2004 (not July 1, 2004 as previously announced). The *Act* comprises two parts. The first deals with the protection of personal health information. Section 31 of that part expressly deals with fundraising, which at first instance had a fairly restrictive consent provision. Bill 159 also had a "fundraising section." Section 26 provided that consent was required before personal information for marketing or fundraising purposes could be disclosed (except under specific conditions, e.g., if the patient is given written notice and does not opt out).

In the original draft, section 31 required a health information custodian (as defined) to obtain the express consent from an individual to collect and use his or her personal health information for fundraising purposes. In the clause-by-clause process and consultation period, the provisions of one section were moderated (with the addition of 31(1)(b)) so that it presently reads as follows:

> 31(1) a health information custodian may collect, use or disclose personal health information about an individual for the purpose of fundraising activities only where;
>
> (a) the individual expressly consents; or
>
> (b) the individual consents by way of implied consent and the information consists only of the individual's name and prescribed types of contact information.

It is also expected that there will be regulations to the legislation that will provide guidance to the phrase "prescribed type of contact information." There has been some suggestion that this term will likely be limited to include the individual's mailing address but not certain other contact information such as e-mail address.

The Ontario government continues to work with stakeholders to address the remaining issues, and there is expected to be a further round of public consultation on the proposed regulations. It is also hopeful that, to the extent it deals with personal health information, the *Health Information Protection Act, 2004* will be designated "substantially similar" to PIPEDA.

Ontario is otherwise governed by the *Freedom of Information and Protection of Privacy Act* and the municipal *Freedom of Information and Protection of Privacy Act* handled by the Information and Privacy Commission of Ontario.

Other Provinces

None of the other provinces have enacted private sector privacy legislation per se and, as such, if a commercial activity is involved, PIPEDA applies. However, each province has enacted public sector legislation.

Manitoba

Manitoba is governed by a *Freedom of Information and Protection of Privacy Act.* The government agency responsible for the oversight is the Ministry of Culture, Heritage and Tourism, Information Resources Division. This statute is under review designed to obtain feed-back on how it has worked over the past five years. Manitoba has also enacted a *Personal Health Information Act*, which underwent its five-year review process recently and is presently seeking public input. Manitoba Health is the government body responsible for this statute. In June 2003, the office of the Ombudsman started to selectively post summaries of access and privacy cases on its Web site. Manitoba is in the

beginning stages of developing privacy legislation "substantially similar" to PIPEDA.

New Brunswick

The *Protection of Personal Information Act* came into force in April, 2001, the text of which can be found at the government's Web site. The Ombudsman is responsible for this statute [(506) 453-2789].

Newfoundland and Labrador

Newfoundland and Labrador is subject to a *Freedom of Information Act* and a *Privacy Act*, both of which are regulated by the Department of Justice.

Nova Scotia

Nova Scotia's current privacy law is the *Freedom of Information and Protection of Privacy Act,* a law overseen by the Freedom of Information and Privacy Review Officer.

Prince Edward Island

In PEI, the *Freedom of Information and Protection of Privacy Act* received Royal Assent on May 15, 2001 and came into force on November, 2002. The province has a Web site devoted to this legislation.

Saskatchewan

Saskatchewan is subject to the *Freedom of Information and Protection of Privacy Act,* and the *Local Freedom of Information and Protection of Privacy Act,* oversight of which is handled by the Information and Privacy Commissioner of Saskatchewan. There is also a *Health Information Protection Act, 2003,* proclaimed in force September 1, 2003. The Regulations, still in draft form, involve options allowing the disclosure of patient lists for fundraising purposes. This includes the June 2003 amendments enacted in the *Health Information Protection Amendment Act, 2003*. Saskatchewan Health is responsible for this statute.

Yukon

Yukon is subject to the *Access to Information and Protection of Privacy Act* regulated by the Ombudsman and Information and Privacy Commissioner of the Yukon.

PART II: EFFECTS OF PRIVACY LEGISLATION ON CHARITIES AND NONPROFIT ORGANIZATIONS

There are some key issues facing organizations regarding the protection of personal information as it relates to charitable and not-for-profit organizations. One revolves around the definition of "commercial activity" and another

around the issue of "consent." And there are differences depending on whether or not PIPEDA, the Alberta PIPA, the BC PIPA, or none of the above apply.

Federal

The application of PIPEDA to a charity is open to constitutional challenge. As the federal government relied upon its "trade and commerce" power under section 91 of the *Constitution Act, 1867* in instituting PIPEDA, it limited its application to personal information collected, used, and disclosed in the course of commercial activity. The regulation of charities is clearly with provincial jurisdiction under section 92(7) of the *Constitution Act, 1867*.[37] A charity, therefore, found in general breach of PIPEDA may have a constitutional argument that PIPEDA does not apply.

Despite this possibility, even if PIPEDA passes constitutional challenge, whether the activities of a charity (outside of British Columbia) are caught in a province that does not have "substantially similar" legislation (such as Ontario) depends on the nature of those activities. In order for PIPEDA to apply, the collection, use, and disclosure of personal information must have been in the course of the "commercial activities" of the organization. In turn, this requires a consideration of the definition of "commercial activities" in PIPEDA.

"Commercial activities" is defined broadly as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists." The definition focuses on the phrase "conduct that is of a commercial character" and provides as an example of such conduct the selling, bartering or leasing of donor, membership or other fundraising lists. An interesting choice for the example – as if donor lists were a particular area the government wanted to control.

Past judicial treatment of "commercial activity" in the context of other statutes is not particularly helpful in developing a definition. The typical focus is on the concept of profit, whether actual or intended. However, this is but one factor that may be recognized by the court as stated in *Windsor Essex County Real Estate Board v. Windsor (City)*.[38] In that case the court held that "there is no doubt that an intention to make a profit will be a very important factor in determining whether an activity is a commercial activity, but the lack of it does no automatically prevent if from being so characterized."[39] At a minimum, especially in light of the example given in the definition, which makes a specific reference to "bartering," the scope of "commercial activity" will likely be broader than the concept of "profit."

Defining whether an activity of a charity or not-for-profit organization may be "commercial in character" is not easy given the broad definition that likely encompasses any activity where there is an exchange of consideration.

Other than case law, guidance may also be sought from Industry Canada, which has recently issued updated "questions and answers" as part of its PIPEDA Awareness Raising Tools (PARTs) Initiative for the Health Sector. These comments are not legal advice but provide guidance of Industry Canada's view and, although directed to the health sector, some of the comments have an impact on charities and not-for-profit organizations. For example, one question related to how PIPEDA impacts on the ability of health care facilities to send fundraising letters to patients. The answer given by Industry Canada was that "fundraising, in this context, is not considered to be a commercial activity" and further, that "there would be no impact from PIPEDA on this activity, unless the facility was selling, leasing, or trading the fundraising list for some consideration."

Another question asked in the Industry Canada document was whether different privacy rules apply under PIPEDA for health care activities in different settings. Industry Canada answered "yes" and provided the following comments:

> A key consideration in determining which organization or individual should comply with PIPEDA is who has control of the personal information and whether they are engaged in a commercial activity. PIPEDA does not apply to the core activities of a municipality, public school, university, public hospital, or correctional facility. Public sector legislation and provincial health information acts would apply in some cases and in some jurisdictions.

Industry Canada then stated that the application of PIPEDA was based on the nature of the activity (transaction) rather than the nature (public, private, commercial, nonprofit, etc.) of the health organization, institution, or agency:

> A not-for-profit organization can be engaged in a commercial activity to which PIPEDA would apply. For example, the sale of a fundraising list by a charity can trigger the application of PIPEDA with respect to that particular transaction. PIPEDA would not apply to a provincially funded hospital. Hospitals are beyond the constitutional scope of PIPEDA as their core activities are not commercial in nature. A similar argument could be made for charities. Charging for a private room would not bring a hospital within the scope of PIPEDA because the transaction is part of the hospital's core activities, i.e., providing accommodation.

From these comments, it appears that some activities carried on by a charity or not-for-profit organization may be considered to be "commercial activity" to which PIPEDA will apply. The comments also suggest, however, that not every exchange for consideration will be considered to be a "commercial activity." The activity involving an exchange for consideration will likely not be considered "commercial," according to Industry Canada, where the transaction is part of the organization's core non-commercial activities, other than the sale, bartering, or leasing of fundraising lists which will be considered "commercial

activity" by definition, regardless of whether it is a core or non-core activity of the organization.

On the issue of fundraising or donor lists, PIPEDA specifically applies. Therefore it is important to analyze the type of information collected and to determine whether the organization can be seen to be engaged in the sale, bartering, or leasing of such lists. If so, the organization should assume PIPEDA applies. And if so, this becomes an issue of consent. The activity of selling, bartering, or leasing fundraising lists is not prohibited per se – it just means that consent must be obtained prior to collection and, given the nature of the example, expressed consent would be preferable.

These answers seem to draw a fine line in the sand and do not provide much guidance as to the meaning of "some consideration." However, where value is exchanged, fundraising activities such as fundraising dinners, raffles, and lotteries would likely be considered "commercial activity" on the assumption that "fundraising" is a core activity similar to the carrying on of a related business by a charity (such as retail or online sales).

It is generally accepted that "commercial activity" covers for-profit activities. However, the courts may interpret "commercial activity" to include any transaction that involves an exchange, especially in light of the inclusion of the concept of "bartering." Therefore, the cautious approach had been to advise that an organization should assume that PIPEDA applies to charity or not-for-profit organizations engaged in activities involving an exchange of consideration that collect, use, or disclose personal information regardless.

However, the Privacy Commission (in response to the confusion and numerous inquiries) has recently attempted to provide guidance on this issue. In February 2004, the Commissioner issued a Fact Sheet responding specifically to the application of PIPEDA to fundraising and other charitable activities. While helpful, it does not provide guidance on the more difficult questions. For example it states that nonprofit status does not automatically exempt an organization from the application of PIPEDA and that, generally, fundraising is not a commercial activity, but that it may be in the context of golf clubs and athletic clubs. It does not discuss the more difficult questions of the applicability to a fundraising dinner or ball. The relevant excepts include:

> Whether or not an organization operates on a non-profit basis is not conclusive in determining the application of the Act. The term non-profit or not-for-profit is a technical term that is not found in PIPEDA. The bottom line is that non-profit status does not automatically exempt an organization from the application of the Act.
>
> Most non-profits are not subject to the Act because they do not engage in commercial activities. This is typically the case with most charities, minor hockey associations, clubs, community groups and advocacy organizations. Collecting membership fees, organizing club activities, compiling a list of members' names and addresses, and mailing out newsletters are not considered commercial activi-

> ties. Similarly, fundraising is not a commercial activity. However, some clubs, for example many golf clubs and athletic clubs, may be engaged in commercial activities which are subject to the Act.
>
> As the definition of commercial activity makes clear, selling, bartering or leasing a membership list or a list of donors would be considered a commercial activity. As a result, consent is required for the disclosure of this information. Assuming this information would be not considered sensitive, an organization could use a clear, simple and easy to execute opt-out process as a means of obtaining consent.

In the United States, the Maryland District Court upheld the applicability of the Federal Trade Commission's Telemarketing Sales Rule to professional fundraisers working for a charity (see <http://www.ftc.gov/2004/03/nfb.htm>). While the decision is based on American constitutional issues, it is an indicator of the concern that the courts have with activities that infringe on the privacy of the individual, no matter how well intentioned.

Quebec

As this provincial law has been found substantially similar, it supercedes PIPEDA and applies to charities and not-for-profit organizations in Quebec.

Alberta

The Alberta PIPA has a separate Part and special rules for "non-profit organizations" as defined in that legislation.[40] This legislation only applies to the personal information that is in the custody or control of a nonprofit organization if it is collected, used, or disclosed by the organization in connection with a "commercial activity" carried out by the nonprofit organization. Like PIPEDA, the Alberta PIPA states that "commercial activity" means:

> Any transaction, act or conduct or any regular course of conduct that is of a commercial character, and, without restricting the generality of the foregoing, includes the following:
>
> - selling, bartering, or leasing of membership lists or of donor and other fundraising lists,
> - the operation of a private school or early childhood services program as defined in the *School Act*,
> - the operation of a private college as defined in the *Colleges Act.*

"Non-profit organization" is defined as an organization that is incorporated or registered under specified Alberta legislation (i.e., the *Societies Act, Agricultural Societies Act* or registered under Part 9 of the *Companies Act)* or that meets criteria established by regulation. An organization that operates in Alberta as a nonprofit organization that is not covered by the definition in the legislation may not be subject to the Alberta PIPA.

The Alberta PIPA states it does not apply to a nonprofit organization or any personal information that is in the custody or under the control of a nonprofit

organization, subject to section 56(3). Section 56(3) states that the legislation does apply where the nonprofit organization collects, uses, or discloses personal information in connection with any commercial activity carried out by the nonprofit organization. Therefore, in a somewhat circular fashion, the applicability of the Alberta PIPA depends upon whether the organization is involved in "commercial activity" as defined.

The Alberta PIPA is likely a better fit for charities than PIPEDA. For one thing, there is a great deal of latitude and discretion provided by the language of the Alberta PIPA.[41] As with PIPEDA, donor information collected by charities is only covered by the Alberta PIPA wherein it is used for "commercial activity." Commercial activity is taken to mean an exchange, not necessarily creating a profit. However, no definition is provided in the Alberta PIPA and the term will be determined over time by the Office of the Information and Privacy Commissioner acting on complaints.

Further, the Alberta PIPA allows for grandfathering of information for the purposes of consent, which PIPEDA does not. Thus, personal information collected and stored prior to January 1, 2004, is "deemed to have been collected with consent" and may be used for the purposes originally intended. In other words, charities and nonprofit organizations will not have to contact every current or past member, donor, or ticket buyer, to request consent to have personal information in the data base. The existing information does not need to be "recollected." However, in order to continue to use or disclose this information for additional purposes, consent is required. To comply with this requirement, some organizations ensure their stakeholders know what is done with the information, to whom it is disclosed, and provide the option to object to these ongoing uses or disclosures.

British Columbia

The situation in British Columbia under the BC PIPA is significantly different for charities and not-for-profit organizations. Unlike PIPEDA and the Alberta PIPA, the BC PIPA does not focus on "commercial activities" and the application of the BC PIPA is not restricted to commercial activities. Rather, the BC PIPA applies (subject to the exceptions) to "every organization" and to the collection, use, and disclosure of personal information regardless of the nature of the organization or activity and therefore covers both for-profit and not-for-profit organizations in British Columbia.

Further, the exceptions are fairly limited. Not caught by the BC PIPA is personal information that is collected, used, or disclosed:

- for personal or domestic purposes;
- for journalistic, artistic, or literary purposes;
- if PIPEDA applies;
- if the *Freedom of Information and Protection of Privacy Act* applies;

- in certain documents and records related to the courts and judicial administration; or
- that has been collected on or before the BC PIPA came into force.

Therefore, the question of what is "commercial activity" is not relevant to activities of charities and not-for-profit organizations in British Columbia to which the BC PIPA applies. Under this legislation, charities and not-for-profit organizations operating in British Columbia (regardless of the location of the organization's headquarters) are in the same position as for-profit organizations and subject to the legislation in respect of all their activities, not simply to any potential "commercial activity."

Multi-Jurisdictions

Although the impact of operating in more than one jurisdiction in Canada is under review by the offices of the Privacy Commissioner of Canada, British Columbia, and Alberta (with a view of avoiding overlapping enforcement), the issue of which legislation governs, if at all, is a concern for those organizations operating in more than one province. This is especially noteworthy for organizations operating in British Columbia, given that the BC PIPA is broader in scope than both PIPEDA and the Alberta PIPA.

As of January 1, 2004, where a privacy law has been deemed substantially similar to PIPEDA, organizations will be subject to the provincial privacy law as opposed to PIPEDA. However, should any personal information cross a border as part of a commercial transaction, the organization is expected to abide by PIPEDA. This leads to the question of examining the nature of the activities undertaken.

When advising charities and not-for-profit organizations on the application of privacy laws, one should ask the following questions:

- Does the organization engage in commercial activities?
- Does it operate (commercially or non-commercially) in Alberta, British Columbia, and Quebec?
- Does any personal information cross borders (e.g., is it shared among regional offices)?
- Was the personal information collected prior to January 1, 2004?
- Does the activity involve fundraising lists?

The recommended advice to a business to ensure that it is compliant with more than one law is to comply with the law with the higher standard. Similarly, the recommended best practice for an organization operating in more than one jurisdiction is to strive to comply to the highest standard.

However, on March 11, 2004, the Privacy Commissioner of Canada issued a letter to the BC and Alberta Information and Privacy Commissioners regarding how she would deal with the concurrent jurisdiction that exists until the

legislation in those provinces is declared substantially similar and PIPEDA no longer applies to the collection, use, or disclosure of personal information within those provinces. Essentially, until the anticipated exemption is granted and relevant files will have to be transferred, the Commissioner will advise complainants of the option of complaining to the provincial Commissioner. A significant piece of information revealed by the letter is that it appears the Commissioner anticipates that the BC PIPA and the Alberta PIPA will be considered "substantially similar" by the federal government.

Consent and Sensitivity

Consent and sensitivity are two issues facing most organizations once the decision to comply with privacy legislation has been made. The concept of "sensitive information" is important for determining the appropriate form of consent to be obtained and the appropriate degree of security required to protect the personal information. Obtaining the appropriate form of consent, either explicit or implicit, is the key to compliance with PIPEDA. If the consent is defective, then all uses of the personal information, whether properly protected or not, are a breach of the legislation. Further, as security measures are among the more expensive requirements of PIPEDA, the choice of the appropriate degree of security is equally important.

The concept of "sensitive information" is not defined in PIPEDA. However, Paragraph 4.3.4 of the Schedule states:

> Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context.

The next paragraph goes on to specify that the "reasonable expectations of the individual" are also relevant in obtaining consent. Therefore, concerns about the sensitivity of different types of information vary and depend on subjective factors such as age and culture.[42] For example, differences between the attitudes of Europeans and Americans to the role of government in their lives exacerbated the negotiations over the Safe Harbour proposal for American compliance with the E.U. Data Directive. While Europeans believe that government has a duty to protect the privacy of its citizens, they find questions regarding political affiliation or ethnicity objectionable. Americans, on the other hand, answer these questions regularly, but are sensitive about financial disclosure and have an inherent distrust of government's ability to protect their rights.

Other jurisdictions have generally specified certain types of information as being generally "sensitive" and have built in protections, such as requirements for explicit consent or special handling. For example, section 2 of the United Kingdom's *Data Protection Act, 1988* defines "sensitive personal data" as personal data consisting of information pertaining to:

- racial or ethnic origin,
- political opinions,
- religious beliefs or other beliefs of similar nature,
- whether a person is a member of a trade union (within the meaning of the *Trade Union and Labour Relations Consolidation Act 1992*),
- physical or mental health or condition,
- sexual life,
- the commission or alleged commission of any offence, or
- any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Section 4 of the *Data Protection Act, 1998* then refers to data protection principles that are set out in schedules. Schedule 3 applies only to sensitive personal data and requires that the data subject has given explicit consent to the processing of such data.

Australia has a similar list of prescribed types of sensitive information that also includes information about the individual's "…lifestyle, character or reputation."[43] Organizations are prohibited from collecting such information unless they obtain consent. However, there is an exemption for nonprofit organizations that have only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims. These organizations may collect sensitive information about their members or other individuals with which they have regular contact if, prior to collecting the information, the organization undertakes to the individual that the information will not be disclosed without the individual's consent.

In the Spanish *Ley Organica* 15/1999[44] Article 7 sets out what is "specially protected" data. In this statute, the list is first divided according to those items, such as ideology, religion, or beliefs, which are protected under the Constitution. These require the highest level of explicit consent. There is then a further category which includes data that will reveal ideology, union affiliation, religion, or beliefs, for which there are certain exceptions for the maintenance of lists by unions, political parties, churches, and other such groups. Personal information having reference to racial origin, health, and sexual life can only be collected when, for reason of public policy, it is made possible by a law or by express consent. Finally, it is prohibited to create data files for the exclusive purpose of revealing the ideology, union affiliation, religion, beliefs, racial or ethnic origin, or sexual life of an individual.

Similarly, Article 31 of the French *Loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* prohibits maintenance of data files that will reveal racial origins, religious, philosophical or political opinions, or union affiliations, or "…les moeurs…" of individuals without the express

agreement of the individual. However, the maintenance of membership lists by groups such as churches, political parties, and unions is specifically allowed.

Section 28 of Germany's *Bundesdatenschutzgesetz*[45] sets out certain conditions for the storage, communication, and use of data for an organization's own purposes. Previously some protection was given to sensitive personal information such as health matters, criminal offences, administrative offences, religious or political views, and trade union status. Effective May 23, 2001, the *Bundesdatenschutzgesetz* was amended to include all of the categories of sensitive information contained in Article 8 of the E.U. Data Directive.[46] Now the collection of such data must be expressly approved by the data subject, and its processing requires a prior review by a data protection official.

From these examples, it can be seen that many democratic countries regard information about an individual's religious, political, or philosophical beliefs as sensitive and restrict its collection, use, and disclosure.

Similar generally sensitive areas may be inferred in Canada from an examination of those rights and values that are specifically protected by law. If such rights and values have been given special protection, the collection of information about the exercise of that right or expression of that value may inhibit the exercise of the right or expression of the value. Accordingly, the information may be considered "sensitive" as that term is used in PIPEDA. For example, to safeguard the freedom to vote according to one's own belief or conscience,[47] Canada uses secret ballots. Privacy or secrecy is considered key to the protection of the right to vote according to one's own conscience. The collection of information, therefore, on how people actually voted may be considered sensitive and require consent (assuming commercial activity).

Section 2 of the *Canadian Charter of Rights and Freedoms*[48] provides a list of fundamental freedoms:

- freedom of conscience and religion;
- freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;
- freedom of peaceful assembly; and
- freedom of association.

Further, section 51(1) provides that every individual is equal before and under the law without discrimination, including discrimination based on race, national or ethnic origin, colour, religion, sex, age, or mental or physical disability.

Any collection, use or disclosure of personal information dealing with these characteristics would most likely be regarded as sensitive because, if the information is used for the wrong purposes, such use would most likely violate

the freedoms or rights that the individual has under the *Charter.* Not all the rights provided in the *Charter,* however, would be equally sensitive.

It is suggested that "sensitivity" will be based on the abilities of others to use such information to take any action harmful to the interest of the individual. For example, usually the sex of a person can be determined by simple observation or inferred from the name. Therefore, a list of names identifying such persons as male or female may not be considered particularly sensitive. However, a list of the names and addresses of the attendees at a local synagogue or mosque, or of the members of the Catholic Church who are also active in Campaign Life, would be most likely considered more sensitive. For these reasons, almost all information collected by religious charitable organizations in Canada would most likely be considered, to some degree, "sensitive information" within the meaning of PIPEDA. Thus, such organizations should consider (assuming commercial activity) collecting, using, and disclosing all of their membership and other information only with the explicit, specific, and written consent of the individual concerned and with the purposes for which such information will be used or disclosed clearly identified.

However, the Commission of Alberta has tried to clarify the question of how the Alberta PIPA affects nonprofit organizations with respect to collecting information for golf tournaments and other fundraising activities. The response was:

> Non-profit organizations as defined in the PIPA Act (Section 56) will only be covered by PIPA to the extent that personal information is collected, used, or disclosed during a commercial activity. The term "commercial activity" has had little interpretation, but generally is defined as any transaction, act or conduct that is of a commercial character (such as selling, bartering or leasing of membership lists, charging fees for counseling services and so on).
>
> For example, if a non-profit organization is charging fees for a golf tournament, the information that is collected, used and disclosed may be subject to PIPA. Generally, this means that the non-profit organization would need to follow the rules under the Act when it comes to notifying the individuals of what information is being collected, what it will be used for and who it may be disclosed to. The individuals may be required to give their consent for the uses and disclosures, and their information may not be used for any other purpose, unless they give their consent.

PART III: STRATEGIES FOR COMPLIANCE

It is a common practice, especially for those organizations outside of Alberta and British Columbia, to advise that if the application of PIPEDA is currently legally uncertain to review the provisions of PIPEDA for the standards set for the protection of personal privacy and to determine whether the organization should or could adhere to those standards. That evaluation would also necessarily consider the implications of not complying with those standards.

Charitable and not-for-profit organizations should first make a decision as to whether provincial legislation and/or PIPEDA applies and/or whether to comply with privacy principles in general. While it is not clear that PIPEDA applies to charitable organizations even if the organization has ancillary "commercial" activities, there are several reasons why, in any event, it may be prudent to comply. These reasons include:

- Canadians are concerned about their privacy and, out of respect for their concerns, steps should be taken to comply with privacy standards.
- PIPEDA may apply if the organization transfers the personal information inter-provincially or internationally.
- PIPEDA and/or a provincial law may or will apply in the near future and there are generally no provisions allowing the use of personal information already collected, so it may be best to start getting consent now.
- Compliance costs are generally lower if the files on each individual are set up in advance to efficiently capture the information on use and disclosure that must be provided to fulfill an access request.
- The reasons for not complying now, if the organization has a choice, are usually related to the cost of implementation and/or the restrictions on certain types of fundraising or other activities that may result.
- Canadians are not so sophisticated as to accept the distinction and argument that PIPEDA (or a provincial statute, for that matter) does not apply because the activity was not "commercial in nature"; Canadians expect protection of their personal information.

To generally assist organizations in complying with PIPEDA, the Office of the Privacy Commissioner has prepared various guides[49] (some are available online). And although Ontario has not yet passed a private-sector privacy law, the Office of the Information and Privacy Commissioner/Ontario has developed a "Privacy Diagnostic Tool (PDT) Version 1.0 Workbook," also available online. And, of course, many law firms and other consultants have also developed guides.

Most of these guides set out similar suggestions on how to proceed with compliance once the decision has been made to take steps to protect the personal information in the organization's possession. These suggestions include:[50]

1. Appoint a Compliance Officer

The first step is to put someone in charge of the process or at least to appoint a co-ordinator and designate that person the compliance officer as required by Principle 1 of the Schedule to PIPEDA and the provincial legislation. This individual should obtain copies of the relevant legislation and regulations, and establish knowledgeable legal and other support. The individual should then

consider assembling a team to oversee and/or conduct the audit and the implementation steps (discussed later).

The privacy compliance officer should then develop a draft plan to implement policies and practices for compliance to be finalized after the conduct of the audit. The plan would:

- implement policies and procedures to protect personal information;
- establish procedures to deal with complaints, inquiries, and retention of information;
- train staff and communicate to staff information about the organization's policies and practices;
- develop information and explain the organization's policies and procedures; and
- ensure the accuracy of the personal information held by the organization.

2. Conduct a Privacy Audit

The next step is usually to conduct an audit. The purpose of the audit is to establish what personal information is currently being collected, used or held, or disclosed by the organization, and how is it currently stored and protected. To perform the audit, the organization's staff will have to become familiar with some of the problems with the definition of "personal information." One area of concern is whether information produced by an individual performing a job function for an organization is personal information. In some European countries, the answer is definitely yes. In Canada, the answer appears to depend upon the balancing of the individual's right to privacy and the needs of organizations, as set out in Section 3 of PIPEDA.[51]

The audit should also identify all jurisdictions where personal information is being collected, as it may be necessary to comply with privacy laws in other provinces or countries.

Particular care should be taken to identify personal information that is disclosed to subcontractors such as: employee information to payroll services, marketing information to ad agencies, information submitted online to service fulfillment providers or data analyzers, lobbying information to trade associations, and mailing information to outside mailing firms. Copies of the contracts with each subcontractor should be reviewed with respect to privacy protection.

Charities and not-for-profit organizations may have special problems in conducting a privacy audit. For example, what is the effect of linking or combining personal information from more than one list or with demographic data? This may increase the sensitivity of the personal information. If fundraising lists are to be traded, then the organization will need to know more about the purposes for which the other organization will use the personal information in order to prepare the appropriate consent form. Further, when is a fundraising activity

wholly charitable and when is it commercial? One guide to answering this question may be whether or not a charitable receipt can be given for the activity.

3. Develop a List of Approved Purposes

A list of approved purposes should be developed. After having conducted the audit, the organization should then examine the purposes for which information is collected, and the nature of the information collected, to determine the organization's long term policy with regard to those purposes and the type of information that is truly necessary to fulfill them. Many organizations have discovered that they are collecting more information than is reasonably necessary.

The list of approved purposes will become the basis for drafting not only the official privacy policies and guidelines, but also the various consent forms that will be used, or other methods of collection.

4. Prepare Privacy Policies, Brochures, and Consent Forms

Once the approved purposes have been identified, the next step is to prepare the organization's privacy policies and guidelines. The privacy brochures mentioned in Paragraph 4.8.2 of the Schedule to PIPEDA, as well as the privacy statements necessary to comply with PIPEDA, must be prepared.

At this stage, the preparation of consent forms or other collection methods will require decisions about the degree of consent and disclosure required based on the sensitivity of the personal information being collected.

5. Consider a New Filing System

As part of this process, internal organizational concerns should be examined. Experience in other jurisdictions, such as Quebec, has shown that one of the keys to low-cost compliance with access requests is having a filing system that segregates the personal information on each individual according to the purpose for which the information was collected, yet has links and controls on the setting up of new files with respect to any individual. If files are computerized, this generally means that the databases in membership and other areas should be linked. The experience in the United States with respect to the *Gramm-Leach-Bliley Act, 2001* has suggested that where this linking is not done, or cannot be done, compliance will be lower and costs will be higher.

Not all purposes require the collection of equally sensitive personal information, and if all information regarding an individual is in one file, then that file must have safeguards appropriate to the most sensitive aspect of the file. If an access request is made and there are no grounds for denying access to one portion of the file, then the file will have to be reviewed item by item to determine what must be severed and what may be disclosed to the individual.

6. Initiate the Privacy Plan

Next, the decisions made by the organization will need to be implemented. Implementation is often co-ordinated so that the organization is comfortable that, from a certain date forward, the organization generally complies with the privacy requirements. It is also necessary to review existing files containing personal information and to either ensure that there is appropriate consent for the retention and use of the information, or that the information is safely deleted. This often requires a mailing to, or other communication with, individuals to announce and explain the new privacy policy and obtain the new consent.

Implementation may also require changes to any Web sites that the organization has to ensure, among other things, that persons using the Web site have access to a copy of the privacy policy or statement every time personal information is submitted. At this point, the required safeguards for the personal information should be in place, whether physical, technological, or in staff policies regarding employee access. The policy regarding the handling of complaints should be ready, as well as the policy on whether to charge any amount to individuals requesting access. Contracts with subcontractors should clearly spell out the compliance measures necessary on their part and provide the organization with a right of audit.

7. Maintain Compliance

Finally, the organization should consider how compliance will be maintained once achieved. Some steps to consider at this stage include:

- Develop policies to ensure that evidence and documentation exists for:
  - each individual's consent, for each database and purpose; and that
  - all uses of, or disclosures from, each database are properly recorded and protected, and are in accordance with the purposes.
- Review databases for accuracy in accordance with the sensitivity of the information.
- Consider separating the responsibility for compliance from the responsibility for collection, use, and disclosure to ensure that collection, use, and disclosure do not proceed without authorization from the compliance officer.
- Provide regular training of new staff and for review and update of the policies.
- Monitor the development and application of provincial laws.
- Monitor transactions with persons outside of Canada for potential breaches of foreign privacy laws.
- Develop a response plan in the event of allegations of a privacy breach.
- Undertake internal or external compliance audits.

The Effect of Non-Compliance

In considering the protection of personal information, it is important to understand the remedies available for breach or non-compliance of the legislation.[52]

Prior to PIPEDA, some Canadian provinces[53] attempted to provide some substance to the common law tort of invasion of privacy. These provinces passed legislation simply providing that it is "…a tort, actionable without proof of damage, for a person, willfully and without a claim of right, to violate the privacy of an individual." However, these statutes have rarely been used.

One reason may be that in each province actions for invasion of privacy must be brought in the superior court of the province, which can be an expensive process.[54] Coupled with this is the uncertainty of recovering damages and the amount of those damages. Damages for this kind of tort would be dependent on the facts in each particular case, and precise estimations would be difficult. However, the increased use of class actions as a form of litigation may change this.

Class Actions

One possible remedy of particular importance to organizations, including charitable or not-for-profit organizations, is the availability of class action suits. Class actions have been a major part of civil litigation in the United States for a long time. They are a more recent, but growing, phenomenon in Canada. Class action suits are available in Ontario, Quebec, British Columbia, and Newfoundland.[55] Class action rules are proposed for the Federal Court of Canada. Although the Federal Court does not yet have rules of procedure that specifically permit class actions, such changes are under consideration. However, as neither the Federal Court nor the Commissioner has exclusive jurisdiction in PIPEDA matters, complainants retain the option of bringing a class action in one of the provinces where they are permitted[56] as a common-law tort. In the provinces that have privacy legislation, recognition of the claim should be assured, and PIPEDA will likely provide a standard for determining whether the organization's conduct amounts to a tort.

Class action legislation varies among the provinces, but Ontario's class action regime is fairly representative. This potential remedy is of particular importance to charities and not-for-profit organizations as it relates to their member or donor lists. As an example, many people have overwhelmingly signed up for the Federal Trade Commission's Do-Not-Call list (including, it appears, some direct marketing executives). A story in DMNEWS (the online newspaper of record for direct marketers) also reported last year that the CRTC is expected to issue a decision on this subject. The Canadian Marketing Association supports and has such a list and the *Commission d'acces à l'information du Québec* has issued a statement emphasizing that telemarketers are to inform individuals of their right to have their name withdrawn from telemarketing lists. With lists that contain at times hundreds or even thousands of individuals, the potential for a breach to result in a class action is high.

The test for class certification in Ontario is articulated in terms that appear broader than the test in the United States. Under the U.S. federal rules, class members must be sufficiently numerous to justify a class action; common issues must predominate; a class action must be superior to other available means of adjudication; and the representative plaintiff's claims must be typical of the claims of the entire class. In contrast, a class action in Ontario requires a minimum of only two plaintiffs; common issues are required, but they need not predominate; a class action merely needs to be a preferable but not necessarily a superior means of adjudication; and the representative plaintiffs' claims need not be typical of the claims of the entire class. Ontario courts also have the flexibility to allow for the creation of subclasses at any stage of the proceedings.

The impact of class action litigation is with the "strength in numbers" effect. Dealing with one complaint would be manageable and containable – dealing with a class of plaintiffs involving hundreds or thousands of complaints would be much more burdensome and expensive. Whereas damages for one individual may be $2,000, multiply that by a hundred or a few hundred individuals and the exposure is suddenly a major concern. Those individuals who might not be bothered to complain may "join the band wagon" if someone else takes the lead. Further, most class action matters are run on a contingency basis with legal fees calculated as a multiple of the damages awarded.

Federal

Partly because of the difficulties of litigation, and in order to comply with the requirements of the E.U. Data Directive, PIPEDA provides that individuals seeking remedies under the legislation may complain to the Commissioner, who must take action (subject to certain exceptions) and report within one year. The Commissioner may also attempt to mediate the dispute. However, the Commissioner has no power to make any decision that is binding on the parties, and in that sense may not adjudicate the dispute. The role of the Commissioner is one of an advocate for the protection of personal information and privacy in Canada, and not that of a dispassionate or specialized adjudicator.[57] For this reason, organizations should carefully weigh the interpretations and pronouncements of the Commissioner.

It must be remembered that Schedule 1 contains both mandatory provisions and discretionary provisions. An organization is obliged to comply with all ten principles, given the use of the mandatory language through the word "shall." However, as the subclauses within the 10 principles use the discretionary word "should," these provisions are recommendations that do not impose direct obligations. Having said that, however, it would be prudent to voluntarily comply with these recommendations, given that section 11(1) of PIPEDA allows an individual to file a complaint against an organization for contravening a mandatory obligation or for not following a recommendation set out in Schedule 1. As such, the Commissioner will investigate an organization for

breaches of the mandatory obligations and for failures to follow the discretionary recommendations.

If an organization fails to comply with PIPEDA's requirements, it can become subject to a complaint. In most cases there is no time limit for filing a complaint, except when access is denied. In this case, the complaint must be made six months after the refusal. Division 2 of PIPEDA outlines the remedies available to an individual where it is alleged that an organization has contravened a requirement under Part One of the legislation. Section 11(1) of PIPEDA provides that an individual may file a written complaint with the Commissioner alleging that an organization has either contravened a Division 1 provision or a Schedule 1 recommendation. The Commissioner may also, under section 11(2), initiate a complaint if it is satisfied that there are reasonable grounds to investigate the matter. Under section 11(4), the Commissioner must give notice to the organization if a complaint under PIPEDA has been filed.

Pursuant to section 12(1) of PIPEDA, the Commissioner must investigate all complaints. The Commissioner has one year from the date of the complaint to prepare a report. Investigators will obtain the information directly, with the interviews conducted in private. The findings of the investigation are disclosed to the parties involved prior to finalizing the investigation. This allows the parties to make additional representations and provides an opportunity to resolve the matter before finalization. There are extensive (despite non-binding findings) powers by which to investigate complaints including:

- summoning and enforcing the appearance of a person to give testimony before the Commissioner (s.12(1)(a));
- administering oaths (s. 12(1)(b));
- receiving and accepting any evidence, by oath, affidavit or otherwise, that the Commissioner deems fit, regardless of whether it would be admissible in court (s. 12(1)(c));
- entering any premises occupied by an organization, other than a dwelling house, at any reasonable time (s. 12 (1) (d));
- conversing in private with any person in any premises entered (s. 12 (1) (e)); and
- examining or obtaining copies of or extracts of relevant materials found in any premises (s. 12(1)(f)).

A complaint will either be *not well founded* (e.g., not enough evidence to indicate a violation of the PIPEDA), *well founded* (there is enough evidence to indicate a violation, *resolved* (the investigation supports the complaint, but the organization agreed to take corrective measures to remedy the situation), or *discontinued* (the investigation is terminated).

The Commission may make public any information relating to the privacy polices and procedures of the organization if the Commission considers that it is in the best interests of the public to do so.

Under sections 14 and 15 of the PIPEDA, a complainant, including the Commissioner, may apply for a court hearing to the Federal Court after the Commissioner's report has been issued,. Therefore, if either the complainant or the Commissioner is not satisfied, either may apply to the Federal Court for a hearing in respect of the matter.

Upon hearing the case, the Federal Court has certain remedial powers as set out in section 16, including:

- an order that the organization correct its practices to comply with sections 5 to 10 of PIPEDA (s. 16(a));
- an order that the organization publish a notice of any action taken or proposed to correct its practices (s. 16(b)); and
- an award of damages to the complainant, including damages for any humiliation that the complainant has suffered (s. 16(c)).

With respect to damages, some guidelines are beginning to develop. For example, the Supreme Court upheld humiliation damages of $2,000.00 for the publication of a photograph without consent.[58] And, in the Spring of 2003, a settlement was reached in one of the Internet unauthorized cookie-tracking cases that provided for potential payments of up to $40.00 U.S. to each individual. The total payments were capped at $1,900,000.00 U.S.[59]

Finally, section 28 under Division 4 of PIPEDA, outlines three statutory offences with which an organization may be charged, including:

- knowingly contravening section 8(8) of the statute, which stipulates that an organization has a duty to retain information until a requester's recourses have been exhausted;
- knowingly contravening section 27.1 of the statute, which prohibits employers from taking action against employees and independent contractors who, in good faith, report contraventions of PIPEDA to the Commissioner, or refuse to participate in activities which fail to comply with the legislation; or
- obstructing the Privacy Commissioner or the Privacy Commissioner's delegate in the investigation of a complaint or in conducting an audit.

These three statutory offences are punishable by summary conviction and a fine not exceeding $10,000.00 (section. 28(a)), or by an indictable offence and a fine not exceeding $100,000.00 (section 28(b)).

Alberta

Enforcement of the Alberta PIPA lies with the Information and Privacy Commissioner appointed by the provincial legislature. The Commissioner has order-making powers including the right to enjoin non-compliant practices. The Commissioner's order is final.[60] An organization has 50 days to comply with the order. Any application for judicial review must be taken within 45 days. A person may seek damages against the offending organization directly in court.[61] Penalties under the Alberta PIPA carry fines of up to $100,000.00.[62] The office of the Information and Privacy Commissioner releases Annual Reports within which statistical analysis, investigative summaries and financial statements are found.

British Columbia

The enforcement of the BC PIPA lies with the Information and Privacy Commissioner appointed by the provincial legislature. The Commissioner has order-making powers including the right to enjoin non-compliant practices. Orders must be complied with within 30 days unless an application for judicial review is made before that date.[63] Further, if the Commissioner makes an order, or if an organization is convicted of an offence under the BC PIPA, that person may seek damages for actual harm in the BC Supreme Court.[64] The penalties under the BC PIPA carry fines of up to $100,000.00.[65]

CONCLUSION

For charities and nonprofit organizations, many of which have limited resources, paying a fine and/or being exposed to an investigation or action can be devastating regardless of which legislation applies or not. And, although some organizations may consider the remedies provided by the PIPEDA to have limited effect, complainants may go beyond PIPEDA.

On a practical note, each organization will need to examine its own structure and activities internally and externally to determine how it will ensure the protection of personal information. While it is also recognized that there is no common solution for privacy compliance for all organizations, it is likely prudent for all organizations to implement the CSA Model Code principles to protect themselves from public complaints and audits, and, for those operating inside Alberta and British Columbia, to ensure compliance with provincial legislation.

REFERENCES

- BC PIPA full text: <www.legis.gov.bc.ca/>
- Office of the Information and Privacy Commissioner/British Columbia: <www.oipc.bc.ca>
- BC Ministry of Management Services: <www.mser.gov.bc.ca/foi_pop/Privacy/default.htm>
- Alberta PIPA full text: <www.assembly.ab.ca/>

- Office of Information and Privacy Commissioner/Alberta: <www.oipc.ab.ca/>
- Alberta Information Management, Access and Privacy Division: <www.gov.ab.ca/foip> (780) 427-5848 see also <www.psp.gov.ab.ca>
- Federal Privacy Commissioner of Canada: <www.privcom.gc.ca>
- Industry Canada: <http://e-com.ic.gc.ca>
- Office of the Information and Privacy Commissioner/Ontario: <www.ipc.on.ca>
- Manitoba Ministry of Culture, Heritage and Tourism, Information Resources Division <www.gov.mb.ca/chc/fippa/index/html>
- Manitoba Ombudsman: <www.ombudsman.mb.ca>
- New Brunswick government: <www.gnb.ca/act/acts/p-19-1.html>
- Newfoundland government/ Department of Justice: <www.gov.nf.ca/just/>
- Nova Scotia, Freedom of Information and Privacy Review Officer: <www.gov.ns.ca./foiro/>
- Prince Edward Island: <www.gov.pe.ca/foipp/index.php3>
- *Commission d'access a l'information du Quebec*: <www.ca.gov.c.ca/eng/index_en.html>
- Office of the Information and Privacy Commissioner/Saskatchewan: <www.saskjustice.gov.sk.ca/legislation/summaries/freedo mofinfoact. shtm/>
- Yukon: Ombudsman and Information and Privacy Commissioner: <www.ombudsman.yk.ca>
- Canadian Standards Association: <www.csa.ca>
- Association of Fundraising Professionals: <www.afpnet.org>
- CBA National Labour & Employment Section newsletter: <www.cba.org/CBA/newsletters/lab-2003/14.asp>

NOTES

1. The other federal legislation (*Privacy Act)* that took effect on July 1, 1983 imposes obligations on some 150 federal government departments and agencies with respect to the privacy rights of Canadians by placing limits on the collection use and disclosure of personal information.
2. L.R.Q., c. P-39.1.
3. Although the former Privacy Commissioner sent letters to Alberta (May 27) and British Columbia (May 7) expressing "very grave deficiencies" that in his view made it "impossible for the federal government to recognize the legislation as 'substantially similar'." It is also noted that these statutes are presently under review and a decision is expected shortly.
4. The other Parts are: Part 2, Electronic Documents; Part 3, Amendments to the *Canada Evidence Act*; Part 4, Amendments to the *Statutory Instruments Act*; Part 5, Amendments to the *Statute Revisions Act*; and Part 6, Coming Into Force.
5. S.C.2000, c.5, as amended by S.C. 2000, c.17, s.97. The Code is now Schedule 1 of PIPEDA – "Principles Set Out in the National Standard of Canada Entitled Model Code of the Protection of Personal Information, CAN/CSA-Q-830-96."

6. Some questions that could be asked include: What personal information do we collect? Why do we collect it? How do we collect it? What do we do with it? Where do we keep it? How is it secured? Who as access to or uses it? To whom it is disclosed? How long is it retained? When is it disposed of? Is the policy available? Is the policy reviewed? Is someone accountable? Are staff trained? Are safeguards in place when information is transferred to third parties?
7. The policies should address these types of privacy issues: define the purposes of its collection; obtain consent, limit its collection, use and disclosure; ensure information is correct, complete and current; ensure adequate security measures; develop or update a retention and destruction timetable; process access requests; and respond to inquiries and complaints.
8. For language used in a bank's account agreement which was commended and the complaint of the language being too broad found to be not well-founded, see Case Summary #263.
9. See Section 9(1) of PIPEDA.
10. See Section 9(3) of PIPEDA
11. For other examples, see Case Summary #221 where the delay was 15 weeks and Case Summary #222 where the delay was 8 weeks. In both cases the finding was that the complaints were well founded and resolved.
12. Paragraph 9.4.9. For a discussion of the interpretation of the provisions regarding costs, see P. Jones, Privacy Law: A New Era, a paper presented to the 12th Annual Meeting of the Canadian Corporate Counsel Association in Halifax, August 21–22, 2000.
13. Priscilla Platt, et al., in Privacy Law in the Private Sector-An Annotation of the Legislation in Canada.
14. L.R.Q., c. P-39.1. Or, the *Act Respecting the Protection of Personal Information in the Private Sector*.
15. L.Q. 1991, c.64.
16. Chapter P - 6.5. The statute has 7 parts: Part 1 Purpose; Part 2 Protection of Personal Information (with 7 Divisions); Part 3 Access and Correction; Part 4 Role of Commissioner; Part 5 Reviews and Orders; Part 6 Professional Regulatory and Non-Profit Organizations; Part 7 General Provisions.
17. Alberta PIPA also applies to personal employee information.
18. Section 2.
19. Section 4.
20. Alberta PIPA also makes reference to a "volunteer work relationship," which is defined as a "relationship between an organization and an individual under which a service is provided for or in relation to or in undertaken in connection with the organization by an individual who is acting as a volunteer or is otherwise unpaid with respect to that service and includes any similar relationship involving an organization and an individual where, in respect of that relationship, the individual is a participant or a student."
21. Section 4(4).
22. Section 8(3).
23. Section 8.
24. Section 9.

25. The *Health Information Amendment Act, 2003* come into here May 16, 2003 with a three-year review scheduled to commence by April 25, 2004. Note, the *Freedom of Information and Protection of Privacy Amendment Act*, 2003 (Bill 28) was enacted following a three-year review with the amendments effective June 2003, with the next legislative review scheduled to commence by July 1, 2010.
26. British Columbia also has a *Freedom of Information and Protection of Privacy Act*, which has been amended (as of May 12, 2003) by the *Freedom of Information and Protection of Privacy Amendment Act, 2003* within the next legislature beginning in the Fall of 2003.
27. The statute is in 12 Parts. Part I: Part 1. Introductory Provisions; Part 2: General Rules; Part 3: Consent; Part 4: Collection; Part 5: Use; Part 6: Disclosure; Part 7: Access; Part 8: Administration, Part 9: Case of Personal Information; Part 10 Role of Commissioner; Part 11: Reviews and Orders;; Part 12: General Provisions.
28. Section 8.
29. Section 8(3).
30. Section 9.
31. Section 18(2)
32. Section 20.
33. Section 30.
34. Sections 23–32.
35. Section 34.
36. Section 35.
37. Which states: "The Establishment, Maintenance and Management of Hospitals, Asylums, Charities and Eleemosynary Institutions in any of the Provinces, other than Marine Hospitals."
38. (1974), 6 O.R. (2d) 21.
39. Note, this decision was overruled on other grounds in Ontario (Regional Assessment Commission) v. Caisse Populaire de Hearst Ltee. (1983), 143 D.L.R. (3d) 590.
40. Part 6, Section 56.
41. For example, the word "reasonable" appears 64 times in the legislation.
42. This next section is modified from Jones, P., "Between God and You: Canada's New Privacy Law," The Philanthropist, Vol. 18, No. 1. (2003). With permission.
43. Privacy Amendment (Private Sector) Act 2000, Act No. 155 of 2000 that came into force on December 21, 2001.
44. Ley Organica 15/1999, de 13 diciembre, de Proteccion de Datos de Caracter Personal.
45. Vom 20.12.199, BGBI. I. S. 2594.
46. Gesetz zur Anderung des Bundesdatenschutzgesetzes und anderer Gesetze, BGBI vom 22.05.2001 S.904.
47. As expressed in Section 3 of the Canadian Charter of Rights and Freedoms, Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act, 1982 (U.K.), 1982, c.11.
48. *Ibid.*
49. See, for example, Office of the Privacy Commissioner, *Your Privacy Responsibilities: A Guide for Business and Organizations* (Ottawa: Office of the Privacy Commissioner, 2000).

50. This next section is built upon portions of Jones, P., "Between God and You: Canada's New Privacy Law," *The Philanthropist*, Vol.18, No.1 (2003). With permission.
51. The Privacy Commissioner of Canada first applied this test in his findings regarding the collection by IMS Health of Information regarding the prescribing habits of doctors without their consent. For a critique of his use of the balance test in that specific case, see Jones, P., "Striking the right balance," *Law Times*, December 10, 2001, p. 7.
52. A frequent question is: what happens if the organization does not comply with PIPEDA and is it worth the cost of compliance?
53. British Columbia in 1968, see the *Privacy Act*, R.S.M. 1970, c.74; Saskatchewan in 1974, See *The Privacy Act*, R.S.S. 1978, c.P.24; and Newfoundland in 1981, see the *Privacy Act*, R.S.N. 1990, c.P.-22. These were based in part of Sections 50 and 51 of the New York Civil Rights Law.
54. See G.H.L. Fridman, The *Law of Torts in Canada, Volume 2* (Toronto: Carswell, 1990) at pages 200–201; and Burns, "The Law and Privacy: the Canadian Experience" (1976), 54 C.B.R. 1 at 38.
55. *Class Proceedings Act* S.O. 1992, c.6; *Code de procedure civile*, L.R.Q., cC-25; b.IX; *Class Proceedings Act*, R.S.B.C. 1996, c.50. On April 1, 2002 Newfoundland proclaimed its *Class Actions Act.* The first statement of claim was filed within a month of proclamation.
56. It should be noted that with its decision in *Western Canadian Shopping Centres v. Dutton*, [2001] SCC No. 46, the Supreme Court of Canada has allowed a broad interpretation of the representative action provisions in Alberta's Rules of Court that may expedite the bringing of class actions in most provinces.
57. See for example Sections 18, 20(2) and 24 of PIPEDA.
58. *Aubry c. Les Editions Vice Versa Inc.* [1991] R.R.A. 421 (Que.), (1996), 71 C.P.R. (3d) 59 (Que. C.A.), [1981] 1 S.C.R. 591 (SCC). A professional photographer had taken a photograph of a young woman sitting on some steps in a public place in Montreal. The photograph was used, without her consent, to illustrate an article in a literary magazine The courts at all levels found that the photograph was in no way derogatory or humiliating to the individual per se, neither in the way the individual was portrayed, nor in any relationship that it had to the text. Damages of $2,000 were awarded at trial. In the Supreme Court the issue was whether there had been sufficient evidence of humiliation damages arising out of the invasion of privacy in order to support the action in tort. There was dissent, and although the award of damages was considered high, the award was upheld. The only evidence of damages was that the young woman had testified briefly that she had some difficulties at school because her friends teased her.
59. Reuters, "Amazon unit settles lawsuit," *Silicon Valley.com*, April 30, 2001.
60. Section 53.
61. Section 60.
62. Section 59(2).
63. Section 53.
64. Section 57.
65. Section 56.