# *PRIVACY LAW AND GOVERNANCE IN THE NON-PROFIT SECTOR*

## *The Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5, and its Impact on Non-Profit Organizations and Charities*

With so much written in the past couple of years and particularly in the past few months, about new and impending privacy legislation, I thought it important to clear up some misconceptions about the various laws and their applicability to the non-profit sector. Being a corporate lawyer, operating within the non-profit sector, I have recently received requests from other charitable and non-profit leaders as to how these laws will affect their organizations. I am not alone. The Office of the Privacy Commissioner, since January of 2001, has received well over 25,000 inquiries. Questions I have been asked include such ones as, "How should we prepare?" and "What will we have to do differently with donor lists?" and "Can our Central Office in one province, communicate private information with offices in different jurisdictions?" With these papers, I will endeavour to answer many of these questions and to give an overview of the increasingly important area.

**The Federal Legislation**

Since January 2001, the federal Personal Information Protection and Electronic Document Act (PIPEDA), Part 1, has been law and has been in effect for banks, the RCMP, CSIS, airlines and airports, railways, telecommunications industries, radio stations and other cross-border undertakings, and similar undertakings for which the federal government has constitutional legislative authority. Also included are certain Crown corporations operating in these areas, such as the CBC. Additionally, the legislation already applies to every non-federally regulated organization that does the following things:

(i) sells personal information that it has collected, used or disclosed in one province outside that province; or

(ii) collects, uses or discloses personal information in connection with the operation of a federally regulated private sector entity (e.g., where Air Canada retains a non-federally regulated consultant to collect personal information from the Airlines' customer list)

On January 1, 2004, the three-year phase-in of the PIPEDA will be complete and will apply the legislation to *most* organizations in Canada, including businesses and even non-businesses that are conducting a "commercial activity". Indeed, the law will impact on the way that certain organizations collect, use and disclose personal information about individuals in the course of daily commercial activities and even in larger one-time transactions such a business acquisitions.

Understanding the applicability of the federal legislation is a matter of appreciating the federal-provincial division of powers. Some matters are reserved for the exclusive legislative domain of the federal government, some for the provincial governments. Is your organization federally or provincially regulated?

Note that there are serious constitutional law issues about the extent that the federal government has the authority to regulate privacy in a province. For the purposes of these papers, federal authority is assumed.

The phase-in of the federal PIPEDA was designed to allow the provinces to put their own legislation into place. As of date of writing, only the Province of Quebec has actually enacted legislation. British Columbia and Alberta have drafted and even introduced Acts into their legislative process. They may become law before January 1st. Ontario has a draft Act, but its process has been interrupted by the provincial election. The Ontario draft law would have made some substantial changes, but it is highly unlikely that there will be law before the election in October. So, it may likely be changed again. Thus, analysis of the privacy law in this province must of necessity focus on the federal PIPEDA. Does any part of it affect your non-profit organization? If so, how?

**The Law**

The PIPEDA enacts into law ten general principles contained in the Canadian Standards Association's Model Code for Protection of Personal Information. It contains these ten principles that are to be applied to commercial activities even now. They are as follows:

1. ***Accountability*** **–** An organization is responsible for personal information under its control (and, importantly, this includes third-party processors such as mailhouses, and fundraisers) and shall designate an individual who is responsible for the organization's compliance with the law. The legislators call this person the "Chief Privacy Officer". This person will have to understand policies procedures and deal with complaints. In my opinion, this person should not be a junior person.

2. ***Identify Purposes*** **–** The purposes for which the information is collected should be identified by your organization at or before the time the information is collected. I can provide precedent "Purpose Statements" for organizations. They should be tailored to each organization so that they fit an organization's mission or business. Simply filling in a template will not be the best approach, as purpose, use and consent levels are best linked.

3. ***Consent*** **–** This may very well be the heart of the PIPEDA. The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, "except where inappropriate". Note here that PIPEDA replaces "except where inappropriate" with specific exceptions, such as, for law enforcement, emergencies and for scholarly and research purposes. Reference must be made to PIPEDA here.

Reliance on the CSA Principles is not recommended. Your organization would be well advised to know that consent could be given in various ways, including express and implied consents. The way in which an organization seeks consent may vary depending upon the circumstances and the type of information collected. An organization should seek express consent when the information sought is sensitive (medical, grades, financial).

Consent may be given in various ways. An application form may be used to seek consent, collect information and inform the individual of the use(s) that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses. A check off box may be used to allow individuals to request that their names, addresses and other information not be given to other organizations. Those who do not check it are assumed to consent to use for this purpose. Consent may be given orally when information is given over the phone.

To date, however, the Privacy Commissioner has required express consent in almost all instances where consent is required – a higher burden on the organization.

All this written, I would advise getting written consent whenever possible and express consent in most situations. Reliance upon implied consent looks likely to prove problematic, given the decisions of the Commissioner so far.

Note also that consents may also be withdrawn at any time!

4. ***Limiting Collection –*** The amount and type of information is limited to what is necessary for an identified purpose. If new purposes develop, new consents are required, too. Naturally, information collection shall be collected by fair and lawful means.

5. ***Limiting Use, Disclosure and Retention of Personal Information –*** An organization can only use, disclose and retain for the purposes for which the information was collected. Information shall be retained only as long as necessary for the completion of those purposes.

   For the purposes of planned giving, the information given will be needed for a long time, in many circumstances. Therefore, it would be wise to explain the need to keep the sensitive information at time of collection and the security measures in place to protect it. Keeping it is essential for its purpose. Disclosure is the key in this circumstance.

   The organization should also publish guidelines for the destruction of information that is no longer of use.

6. ***Accuracy –*** Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is used. This is just good business practice anyway.

7. ***Safeguards –*** Take real steps to prevent the loss, theft, unauthorized access, disclosure, copying and use of personal information. Safeguards should be appropriate to the sensitivity of the information. Relevant staff should sign confidentiality agreements.

8. ***Openness –*** An organization must make its privacy practices and policies concerning management of personal information easily accessible to the public. A Website is the ideal place to set out a purpose statement, as would be Annual Reports and other direct mailings. Planned giving mailings would even benefit from such disclosure, as they are evidence that the organization is trustworthy and responsible, respectful of persons' privacy.

9. ***Individual Access –*** Upon request, individuals are to be informed of the existence, use and disclosure of all of their personal information and be given access to it. Persons may challenge the accuracy of their information and have it changed if it is wrong.

10. ***Challenge Compliance –*** A person shall be able to address a challenge concerning compliance with all of these principles to the designated individual(s) accountable for the organization's compliance. The Chief Privacy Officer's liaison role will activate at this point.

**Purpose and Definitions**

Section 3 of the Act sets out the law's purpose. It reads, "The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information that a reasonable person would consider appropriate in the circumstances".

As one can read, there are many definitions that are necessary in order to understand this law. Additionally note that it refers to "this Part", or Part 1. Part 2 of the Act concerns electronic documents, and will be dealt with in a subsequent paper of mine.

Section 4 of the Act is the Application section of the Act. It sets out that this first part of the Act applies to, "…every organization in respect of personal information that,

(a) the organization collects, uses or discloses in the course of its commercial activities; or

(b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business"

This applicability is limited in certain ways, including by the Federal Parliament declaring in a later Act that said Act applies notwithstanding the PIPEDA.

Section 2 of the Act is the definitions section. There, one can clarify meanings.

"Commercial activity" is defined as, "…any particular transaction, act or conduct…that is of commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists". So, for example, a charity that sold its membership list to a magazine publisher or to another charity would be engaged in commercial activity.

This definition alone is one that will cause great consternation, as entities that would not normally be thought of as undertaking commercial activities as a rule, can engage in single instances of commercial activity and therefore be caught by the Act. Thus, caselaw in Federal Court will be important (again, assuming federal jurisdiction at all).

"Personal information" is defined as, "information that can be used to identify, distinguish or contact a specific individual". Publicly available information would be excluded from the scope of the Act, as it is already "out there" in the public realm.

Another definition with which the reader should be familiar is the term "Grandfathering". It refers to information that is already in your organization's possessions, prior to the enactment of the legislation, such as client, donor or alumni files. Be aware that this existing information will be subject to the same rules as data collected subsequent to the legislation. Lawyers would say that the information will not be "grandfathered". In fact, going even further, if the collection of this information did not comply with PIPEDA requirements (even though PIPEDA did not necessarily *exist* at the time it was collected), organizations may have to *re-contact* individuals to obtain their consent to the collection, use or disclosure of the information in compliance with PIPEDA.

**Governance -Chief Privacy Officer (CPO)– Essential New Oversight**

PIPEDA will require organizations to appoint compliance officers responsible for overseeing the management of the organization's information handling. Upon request, the compliance officer must be identified. Again, I will emphasize that this person(s) should not be a junior employee, but should be one who has a good understanding of the overall activities of your organization, who has experience in change management, who has public relations, negotiation and crisis management skills and who is able to maintain knowledge of the privacy laws and regulations. This person(s) must also be able to communicate with every member of your organization and maintain strict levels of confidentiality. The liaison function with the privacy commissioner's office and with your constituencies is also important.

The CPO need not necessarily be an in-house counsel or chartered accountant (should your organization be large enough to have these persons), but many large institutions have made the CPO role a functional responsibility of these professional ranks. Be prepared to properly train and educate your chosen delegate(s).

**Applicability and Exclusions**

What can one be certain is *not* covered by the legislation? Personal information about *employees* of non-federally regulated organizations is not subject and will not be subject to PIPEDA. Only provincial privacy legislation will apply to those persons.

Some charities may be completely unaffected by the PIPEDA if they do not engage in any commercial activity and they do not engage in cross-border transactions. The act of gathering information about donors in order to solicit them for gifts is not a commercial activity and is not covered by the Act.

It is known, however, that the collection of personal information shall be limited to that which is necessary for the purposes identified. Remember, that before or at the time of collection of information, the organization must document and identify in an easily identifiable way to the individual, the purposes for which it is being collected. (Schedule 4.4, 4.4.1)

When an organization wants to use already collected information for a new purpose, it must document the purpose and obtain a consent for the new use. (Schedule 4.3.1, 4.5.2)

A consent is not necessary for collection of information solely for artistic, journalistic or literary purposes. (Section 7(1)(c))

An entity may disclose personal information without the knowledge or consent of an individual if the disclosure is to a barrister or solicitor who is representing the entity. (Section 7(3)(a))

A business may disclose personal information for the purpose of collecting a debt owed by the individual to the organization. (Section 7(3)(b))
An organization may disclose personal information to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information. (Section 7(3)(c))

As emphasized, an organization must be open about its policies and practices, and said organization must respond to a request by an individual for his or her information within a reasonable time and at minimal or no cost to the individual. (Section 8, Schedule 4.9, 4.9.1, 4.9.4, 4.9.5) Thirty days is usually a maximum response time. In fact, where a person suffers a form of sensory deprivation, a business is obliged to provide personal information in an alternative format, such as by audiotape or in Braille. (Section 10)

Other exceptions to providing access include information that is prohibitively costly to provide, information that contains references to other people, information that cannot be disclosed for legal, security or commercial proprietary reasons and information that is subject to solicitor-client privilege. (Schedule 4.9)

Notably for non-profits and charities, it is well worth re-emphasizing that there is *no exemption* for third party processors. So, for example, third party fundraisers should be made to sign contracts ensuring compliance with PIPEDA with the organization if the organization transfers information to the third party for processing. If the organization fails to get such a contract signed, it risks being liable for the actions of its agent, the third party.

Broad or universal statements of applicability are difficult to make, as individual organizational ties to government are relevant. For example, some private non-profits may be subject to PIPEDA owing to their ties with government. I recommend consultation with legal counsel or with the Privacy Commissioner if questions still exist in readers' minds.

**Conclusion - How Should My Organization Respond?**
**The Privacy Audit**

My best advice is to prepare as if legislation will inevitably apply to your organization. Most generally, this means having a *privacy audit* done to determine your organization's preparedness. This means that it would be wise, initially, to develop a privacy policy. In addition, your organization should be prepared to select a Chief Privacy Officer, to train employees on the company's privacy policy, to develop a procedure for handling requests for access to personal information and for handling complaints. Confidentiality agreements should be drafted for certain key employees to sign.

In the development of a policy, an organization should recognize that fewer individuals believe that organizations are performing adequately to protect their privacy. Consumers want clear and readily accessible policies that are effective in protecting their privacy rights. Consumers want dispute resolution systems, a responsible person to whom they can go to with issues and complaints, and independent audits or verifications of organizations' compliance.

The most important thing that an organization can do to build client, customer or public confidence is to have its public privacy policies vetted by *an independent auditor*. Having a clear policy and a capable individual in charge of privacy policies goes a long way to ensuring confidence also. Independent verification means testing the people, processes, technology and preventative measures, controls and dispute resolution processes that are in place to ensure that a company is following its stated privacy policies. Customers want many things independently verified, such as security procedures to protect personal information, release of personal information only with explicit consent, and maintenance of internal controls to limit access to personal information to proper and legal users.

Your organization will also want its *privacy risks* analyzed. What risks exist? Beyond damage to relationships that bad practice will cause, there are also penalty sections of the Act. There can be charges of deceptive business practice, legal liability as well as liability or sanction from within your governing industry associations. Poor compliance will inevitably result in costs of remedial compliance, costs that would not have been incurred had things been done correctly in the first place. In the non-profit sector, loss of trust is a death knell, particularly for fundraising arms. Businesses will certainly lose profit and value, their very *raisons d'être.*

A later paper will deal with the specific remedies and sanctions that are found in the PIPEDA, as well as with procedures that are in place to settle disputes. Familiarity with this part of the Act is essential to compliance.

The best organizations, be they non-profit or for-profit organizations, recognize that they will want to develop privacy policies that mirror their corporate visions, their business plan, or the needs of their constituencies. They best understand the types of information they are collecting, how they use and share it and whether, in fact, they even really need that information at all. Minimum legal compliance is a failing approach. Proactivity, the anticipation of constituency needs, is always preferable to waiting for bureaucratic rule-making to force organizational decision-making.

***Prepared by:***

***Jeffrey H. McCully***
***Barrister & Solicitor***
***Chair, Ottawa Roundtable, CAGP***
***(613) 230-9743 Telephone***
***(613) 230-2422 Facsimile***
***jmccully@scotmor.ca***