WHAT CHURCHES & RELIGIOUS CHARITIES NEED TO KNOW ABOUT ONTARIO'S ANTICIPATED PRIVACY LEGISLATION

Mervyn F. White, B.A., LL.B.

A. INTRODUCTION

- Recently, Tom Mitchinson, Assistant Commissioner for the Office of the Information and Privacy Commissioner for the Province of Ontario, began a speech to the Sault Ste. Marie Chamber of Commerce with the following sensible statement to businesses in Ontario:

> "The message I'd like to share with you today is that respecting your customers' privacy is good business. It fosters trust and builds consumer confidence. It strengthens brand recognition, increases customer loyalty and, ultimately, delivers competitive advantage.
>
> What can happen if you ignore privacy concerns? You can alienate customers, lose market share and face declining revenue. Privacy has now become an essential part of any business's 'competitive edge'. "[1]

- The message of Mr. Mitchinson is no less sensible for churches and charities operating in Ontario. Respecting adherents' privacy is good business for churches. It fosters trust. If churches should ignore the privacy concerns of adherents, they risk alienating existing or potential sources of financial support as well as a loss of credibility in their communities.

B. PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

1. Overview of PIPEDA

- At present there is federal legislation in place in Canada that attempts to address the privacy concerns of Canadian consumers. The federal *Personal Information Protection and Electronic*

1 Transcript of speech by Tom Mitchinson, Assistant Commissioner Office of the Information and Privacy Commissioner, Ontario made on September 11th, 2002 to the Sault Ste. Marie Chamber of Commerce found at http://www.ipc.on.ca/english/pubpres/speeches/091102tm.htm.

Documents Act (PIPEDA) has been partially in effect since January 1st, 2001, when it initially applied to the personal information of both customers and employees of a federal work, undertaking or business, such as a bank or airline company. As well, as of January 1st, 2001, it also applied to organizations that disclosed personal information across provincial or national borders for consideration.

- On January 1st, 2002, PIPEDA was expanded to apply to organizations already subject to the legislation that also collect, use or disclose personal health information.

- On January 1st, 2004, PIPEDA will be further expanded to apply to all organizations that collect, use or dispose of personal information in the course of all types of commercial activity.

2. Interplay between PIPEDA and Equivalent Provincial Legislation

- If a provincial government had passed a law that is substantially similar to PIPEDA by January 1st, 2004, then the organizations or activities covered under that provincial law will be exempt from PIPEDA in relation to the collection, use or disclosure of personal information within that province. However, PIPEDA will still continue to apply to any trans-provincial or international transfers of personal information that may occur in that province.

3. Application of PIPEDA to Charities and Not-for-Profit Organizations

- It should be noted that PIPEDA primarily regulates the collection, use or disclosure of personal information in relation to commercial activities. There has been some debate regarding whether or not charities or not for profit organizations will be caught within the scope of PIPEDA. Specifically, the issue is whether or not charities or not for profit organizations engage in "commercial" activities.

- Regardless of the outcome of this debate, the Ontario government has clearly indicated its intention to create "made-in-Ontario" privacy legislation that will be applicable to all types of organizations, regardless of whether they are involved in commercial activities. As a result, the Ontario legislation will have application to both charities and not for profit organizations.

C. PRIVACY OF PERSONAL INFORMATION ACT, 2002 (PPIA)

1. Overview of PIPA

- In the spring of 2002, the Ontario government released a draft version of the proposed Ontario privacy legislation, presently entitled the *Privacy of Personal Information Act, 2002* (PPIA).

- The Ontario government has described the purposes of PPIA as being the following:

- to protect individuals' privacy regarding their personal information;
- to govern organization's collection, use and disclosure of personal information; and
- to strike a reasonable and appropriate balance between individuals' privacy rights and the informational needs of organizations.

- Since the introduction of the initial draft version of PPIA, the Ontario government has made numerous revisions to PPIA (at recent count, the Ontario government may be working from draft version 26) and has been working closely with "stakeholder groups", including representatives from the charitable and not for profit sectors, in an effort to make PPIA more palatable to all interested parties.

2. Concerns Raised by the Charitable and Not for Profit Section about PPIA

- Chief amongst the concerns expressed by representatives of the charitable and not-for-profit sector about PPIA were the following:

  - It treated the activities of commercial organizations on the one hand and charities and not-for-profit organizations on the other as being similar in nature, without recognizing the unique relationship existing between donors and adherents and the charities and not-for-profit organizations they support;

  - It failed to adequately strike a balance between the reasonable and legitimate concerns of consumers respecting their personal privacy and the need of charities and not-for-profit organizations to fundraise and communicate their messages to existing and potential donors and members;

  - It did not contain appropriate "implied consent" provisions, but instead required that actual consent be obtained in all situations, regardless of pre-existing relationships; and

  - It did not contain adequate "opt-out" language but instead focused on "opt-in" provisions which were not realistic in today's information driven society.

3. Content of PPIA

- There are certain key principles which are the foundation of PIPEDA, and which were originally enumerated in the Canadian Standards Association *Model Code for the Protection of Personal Information.* Briefly, these principles are

  - Accountability;
  - Identification of Purposes;
  - Consent;
  - Limiting Collection, Use and Disclosure;
  - Retention and Destruction;
  - Accuracy;
  - Security;
  - Open Information Practices;

- Access and Correction; and
- Complaint Investigations.

- These same principles will form the basis of PPIA. However, whereas PIPEDA has the *Model Code for the Protection of Personal Information* actually appended to it, PPIA will actually incorporate the principles into the actual legislation.

- Despite the numerous revisions and consultations with stakeholders, it is clear that PPIA will not only match, but certainly exceed, PIPEDA in its scope. One example of this is that PPIA will apply to all organizations which collect, use and disclose personal information regardless of whether this is done in relation to a commercial transaction.

D. COMPLIANCE WITH PPIA

In order to be in compliance with PPIA, churches in Ontario will have to do the following:

1. Accountability:

- Churches will be responsible for the personal information in their care.

- Churches will be required to name someone to be responsible and accountable for the compliance with PPIA. This person or group will be responsible for facilitating compliance of the church with PPIA and ensuring that every person working for the church is aware of their duties under PPIA.

- Churches will be required to have information practices in place that comply with the requirements of PPIA.

- Churches will be required to "act in conformity" with their own information practices.

- Churches will be required to have processes in place to respond to inquiries from the public about their information practices and receive complaints from the public about any allegations of contravention by them under the PPIA.

- Churches will be required to take reasonable action to investigate complaints, take appropriate measures to answer any complaints, if received, and change their information practices, if necessary.

- Churches will be subject to offences enumerated in PPIA, such as using deception to collect personal information.

2. Identification of Purposes:

- Churches will be required to identify the purpose for which personal information will be collected, used or disclosed, either before or at the time such information is collected.

- Churches will be required to implement information practices that will be mandated by PPIA. These practices will include preparing and making publicly available a written statement regarding when, how and why they collect personal information.

- PPIA will require that churches obtain some type of consent for the collection, use and disclosure of personal information. While it would appear that the final form of PPIA will allow for some form of "implied consent", it will still require that churches clearly define the purposes for collecting, using or disclosing personal information. This is because a consent cannot exist if the person does not know the reason why the personal information has been collected in the first place.

- Churches must do the following to properly identify the purposes for which personal information is collected, used or disclosed:

  - define the objectives behind the collection (i.e. why the information is being collected);

  - determine whether personal information is even required to meet the objectives;

  - determine the minimum amount of personal information that will be required to meet the objectives;

  - identify how the personal information will be used or disclosed;

  - identify and document the general purposes for which the church collects, uses or discloses personal information;

  - describe its information practices in easily understandable terms; and

  - make information concerning its information practices publicly available.

3. <u>Consent:</u>

- The types of consent which churches will be required to obtain from individuals may (and most likely will) change before PPIA becomes law. At present, the only publicly available draft version of PPIA does not allow for "implied consent". However, it is anticipated that "implied consent" will be permitted in certain limited circumstances.

- Regardless, consent will be an integral part of PPIA and in this regard the following basic principles will drive PPIA:

  - Individuals will be entitled to either provide or withhold their consent to the collection, use and disclosure of their personal information;

  - Churches will be required to obtain the consent of individuals to collect, use or disclose their personal information, except in limited circumstances; and

- Churches will not be entitled to use personal information for any purpose other than for which it was originally collected, except with the consent of the individual who gave the information.

- Churches will be required to become familiar with the consent provisions of PPIA and will have to make judgment calls as to what sort of consent will be required.

4. Limiting Collection, Use and Disclosure

- PPIA will place restrictions on the collection, use or disclosure of personal information, even if the required consents have been obtained.

- For example, churches will not be entitled to collect personal information if other information is available which will satisfy their needs. As well, churches will not be entitled to collect personal information simply because a person consents to its collection.

5. Retention and Destruction:

- Churches will be required to destroy personal information in their custody or control after it is no longer required to meet the purposes for which it was originally collected.

- PPIA has specific provisions respecting the retention and destruction of personal information in the care and control of organizations. As such, churches will need to:

  - keep records of all non-consensual uses and disclosures of personal information and retain that information as part of the records respecting that personal information;

  - keep records of personal information used to make decisions about a individual, such as an employee, after the decisions are made, in order to allow that person to access the information; and

  - destroy any records of personal information as soon as they are no longer authorized to retain the personal information.

6. Accuracy:

- Churches that collect, use and/or disclose personal information must take all reasonable steps to ensure that the information is as accurate as is necessary for the purposes for which it was originally obtained

- Churches will also be required to take all reasonable steps to reduce or eliminate any possibility of inaccuracy in the personal information in their care and control.

- Further, churches will be limited in their ability to update any records of personal information, except where such an update will be required to fulfill the purposes for which the personal information was originally collected, where the individual consents to the updating, or the personal information is required or permitted by law to be updated.

7. Security:

- Churches will be required to ensure that sufficient and appropriate security measures are put in place to protect the personal information in their care and control, as well as to ensure that personal information in their care and control is protected against unauthorized use, copying, disclosure or destruction.

- Churches will be required to assess the nature of the personal information in their care and control to determine the extent and type of security that will be required. The more sensitive the personal information held by churches is, the greater the need for security will be, and as a result a higher level of security may be required for some personal information. Churches will be required to disclose the types of personal information in their care and control to the general public as well as the type of security in place to safeguard such personal information.

- Sensitive personal information requiring a higher level of security includes:

  - personal health information;
  - personal income information;
  - credit card information;
  - health card information;
  - information respecting a person's race, religion, sexual preference; and
  - information respecting political affiliations or beliefs.

- It is recommended that churches create a system whereby individuals can identify the level of security that they wish to be used in relation to their personal information. As people will have different ideas about how their personal information should be secured, churches will likely have to have a number of different security levels in place for individuals to choose from.

8. Open Information Practices:

- PPIA will require that churches that collect, use or disclose personal information provide enough information to interested persons for them to know how their personal information will be collected, used and disclosed and to know what their rights are in relation to such collection, use and disclosure.

- PPIA will require transparency by churches about their information practices.

- Written policy statements respecting the information practices of churches are recommended. At a bare minimum, they should contain the following information:

- the name, title, position and contact information of the person who has been named to oversee and implement the information practices of the church;

- the means by which access can be gained to personal information held by the church;

- a description of the type of personal information held by the church; and

- a description of the security measures implemented by the church to protect the personal information in its care and control.

9. Access and Correction:

- Individuals will have a right to access personal information held by churches under PPIA.

- Churches will be required to provide individuals with access to their personal information held by them and the right to challenge the accuracy and completeness of their personal information.

- Specifically, if requested, churches will be required to provide individuals with specific information about how they collect, use and disclose personal information and, upon request, shall also be required to inform the individual of the existence, use and disclosure of their personal information.

- However, the right of an individual to access or correct their personal information will not be absolute. Churches will have the right to review the request to determine whether it is frivolous or vexatious.

- To access or correct their personal information, individuals will have to make written requests.

- Pursuant to PPIA, churches will have to do the following when faced with a request for access to personal information:

  - help prepare the request for access, when requested by the individual;

  - determine if one of the exemptions enumerated in PPIA is applicable and, if so, then access may need to be limited or denied;

  - notify any affected third parties and consider their responses to the request;

  - limit the information disclosed to only that information to which the individual is entitled;

- either provide access to the requested information or provide a written response indicating either the requested information is not in the church's possession or the reasons for refusing access to the information;

- take reasonable steps to ensure that the person requesting access to personal information is the person entitled to it;

- determine if a waiver fee is applicable;

- give a copy of the information to the individual, if applicable; and

- give information on the church's use and disclosure of the personal information to the individual, when requested.

CARTERS
CARTER & ASSOCIATES
BARRISTERS, SOLICITORS & TRADE-MARK AGENT
Affiliated with **Fasken Martineau DuMoulin LLP**

211 Broadway, P.O. Box 440,
Orangeville, Ontario L9W 1K4
Phone: (519) 942-0001

www.carters.ca
www.charitylaw.ca