Privacy Legislation and the Church

Canadian Baptists
OF WESTERN CANADA

Cultivating Leadership. Investing in Relationship. Engaging in Mission.

Table of Contents

The Impact of Privacy Legislation on Churches

Impact of Privacy Legislation on Churches

All churches and non-profit organizations should have a privacy policy as a matter of Best Practice. In British Columbia, it is the law. In all other western provinces and territories, privacy laws do not apply to churches — unless they engage in commercial activities.

Protecting privacy makes sense in any organization that relies on confidentiality and trust in its relationships. The CBWC encourages all churches to adhere to the principles and practices set out in federal and provincial privacy legislation.

Background

In 2004, the federal government introduced privacy legislation to address the issues around the collection, use and storage of personal information for commercial purposes. This law is known as the Personal Information Protection and Electronic Documents Act (PIPEDA). British Columbia and Alberta enacted their own legislation, both called the Personal Information Protection Act (PIPA), the same year. (BC and Alberta also enacted other legislation that applies only to public agencies but have no bearing on churches.)

These laws respond to growing public concern about how private information is gathered, held and used, concerns that have been heightened because of the new capabilities to gather and share information using electronic technologies such as the internet, servers and computers. The legislation protects individuals' personal information from unauthorized access and use while enhancing individuals' rights to gain access to information about themselves.

Since the enactment of federal and provincial legislation, most churches have complied. However, there has been much confusion and misinformation. Must churches follow the same rules as businesses? Can we hold information on a server outside of Canada? Are we allowed to have a church directory? Does national security legislation trump privacy? What information can we collect? What information can we share, and with whom?

This document attempts to clarify what churches can do to protect the privacy of their congregants.

Disclaimer: The following document is a brief summary of legal opinion for the purpose of providing background information. Readers are advised that they are responsible to determine for themselves the requirements and implications of any and all federal, provincial or territorial legislation. This document is not intended as a substitute for legal advice.

The Impact of Privacy Legislation on Churches Continued

Why Do Churches and Non-Profits Need to be Concerned About Privacy?

- As Christians, we esteem and value each individual. One way to express this is by honouring each individual's desire to control their own personal information.
- Congregants expect churches to be safe, secure places where personal information is used only as intended. Protecting privacy is a simple, common courtesy.
- Relationships in churches are complex and change over time, so confidentiality must be respected in ways that are appropriate to the information.
- The capacity of new technologies to share information globally with the click of a button means extra diligence is necessary to protect privacy.
- Everyone has the right to have their personal information protected, to have access to that information and to know and control how it is used.
- In British Columbia, it is the law.

What Does Personal information Include?

Personal information includes both facts and subjective information about an individual:

- Name, gender, race, ethnic origin, marital status, educational level
- Religion
- Political affiliations or beliefs
- Personal e-mail address and messages, IP (Internet protocol) address
- Age, height, weight, medical records, blood type, DNA code, fingerprints, voiceprint
- Income, purchases, spending habits, banking information, credit/debit card data, loan or credit reports, tax returns
- Social Insurance Number (SIN) or other identification numbers.
- Photographs and videos that identify the person
- Opinions about a person (such as held in counselling session**)**

Personal information does not include: (partial list)

- Work emails, address or phone number
- Correspondence, information and documents related to work
- Information that can be found through public sources, like a phone book or website
- Information voluntarily disclosed, such as in a public interview
- There are exemptions for information collected for literary, journalistic and artistic purposes, as well as genealogical research.

Issues Covered by Privacy Legislation

Federal and provincial protection of privacy laws all share the same purpose: to govern the collection, use and disclosure of personal information by the private sector, balancing the right of an individual to have personal information protected with the needs of certain organizations to collect, use and disclose that information.

Federal and provincial laws are founded on the same basic privacy principles relevant to all churches, whether or not the actual legislation applies to them. They include:

- Organizations are accountable to protect personal information under their control.
- The purposes for which the personal information is being collected must be identified during or prior its collection.
- Personal information may only be collected, used or disclosed by an organization with the knowledge and consent of the individual (with limited exceptions as specified in the legislation.)
- The collection of personal information is limited to what is necessary for the identified purposes and will be collected by fair and lawful means.
- Personal information must only be used and disclosed for the purposes for which it was collected, except with consent or as required by law. It can be retained only as long as it is necessary to fulfill those purposes.
- Personal information must be as accurate, complete and up-to-date as is necessary.
- Personal information must be protected by adequate safeguards appropriate to the information.
- Information about an organization's privacy policies and practices must be readily available to individuals upon request.
- An individual has the right of access to personal information about himself or herself and has the right to seek correction. Both these rights are subject to some exceptions as specified in each statute.
- Organizations must provide the means for an individual to challenge an organization's compliance of the above principles.

All churches should strive to meet or exceed public standards in these areas as a matter of Best Practice.

Federal Legislation

Personal Information Protection and Electronic Documents Act (PIPEDA)
PIPEDA is federal legislation came into partial effect in 2001 and was expanded in 2002 and 2004. It determines how private sector organizations may collect, use and disclose information for commercial activities and gives individuals the right to access and correct information held about them.

This legislation can be thought of as default legislation since it applies everywhere in Canada – unless a province or territory enacts its own 'substantially similar' or stronger legislation. In Western Canada, British Columbia and Alberta have enacted their own legislation. In these 2 cases, provincial legislation applies to provincially regulated organizations, including churches. Manitoba, Saskatchewan and the territories do not have their own privacy legislation, so they use PIPEDA.

PIPEDA applies to the personal information collected, used or disclosed by organizations engaged in commercial activities and to agencies under government jurisdiction. If there is no commercial activity, PIPEDA does not apply. This means PIPEDA does not specifically apply to churches or non-profits, unless they are engaged in commercial activities. (Tithing and donations are not considered to be commercial activities. Selling a membership list would be considered to be a commercial activity. Running a daycare for fees, or a school would be considered commercial activity.) However, it is good for churches to be aware of the principles and provisions in the Act so that Best Practices can be
followed.

For more information on PIPEDA, go to:http://www.priv.gc.ca/information/02_05_d_08_e.cfm

Privacy Act
The Privacy Act took effect on July 1, 1983. This Act deals with privacy rights relating to federal government departments and agencies, limiting the collection, use and access to personal information. Individuals have the right to access and correct personal information held by these federal organizations.

Churches are not considered federal government organizations – so the provisions do not apply.

For more on the Privacy Act, go to: http://www.priv.gc.ca/legislation/02_07_01_01_e.cfm

Provincial Legislation

Alberta
Alberta's privacy legislation is overseen by the office of the Information and Privacy Commissioner of Alberta www.oipc.ab.ca

Personal Information Protection Act (PIPA)
Most non-profits and churches are not required to comply with PIPA in Alberta unless engaged in commercial activities; however, churches may choose to comply with PIPA in an effort to adhere to Best Practices. PIPA does not apply to churches if all of the following 4 conditions are met:

- The church is incorporated under Alberta's Society's Act
- The church does not barter, sell or lease membership or client lists
- The church does not engage in any commercial activity.
- The church does not operate:
  - Private schools
  - Early childhood services (as defined by School Act)
  - Colleges (as defined by the Post-Secondary Learning Act)

Under Alberta's PIPA, fundraising, tithes and donations, sending out newsletters or creating member directories are not considered commercial activities.

Despite PIPA, Alberta organizations that engage in commercial trans-border flows of information mustfollow PIPEDA regulations concerning this.

www.servicealberta.ca/pipa/ provides free copies of the Act, a workbook and 10 Steps to Implement PIPA.

Freedom of Information and Protection of Privacy Act (FOIP Act)

The FOIP Act applies to public agencies in Alberta, like government agencies and commissions, boards, universities and colleges. It does not apply to churches, private businesses or non-profits.

www.servicealberta.ca/foip/

British Columbia
BC's privacy legislation is overseen by the Office of the Information and Privacy Commissioner for British Columbia www.oipc.bc.ca

Personal Information Protection Act (PIPA)
PIPA applies to all organizations in BC including churches, non-profits and corporations. It governs how these organizations may collect, use and disclose personal information about individuals. BC's PIPA is very similar to Alberta's PIPA but is considered more strict.

Where the Alberta PIPA does not include churches and non-profits unless they are engaged in commercial activities, BC's PIPA legislation does include churches and makes no distinction between commercial and non-commercial activities.

Provincial Legislation Continued

PIPA requires all organizations, including churches to:

- Get consent for collecting, using and disclosing personal information. Consent must be in a form appropriate to the sensitivity of the information. There are exemptions to consent, such as emergencies, criminal investigations, information required for employment.
- Collect information only for reasonable purposes
- Use and disclose personal information only for the purposes for which consent was given
- Provide individuals with information about the existence, use and disclosure of their personal info and provide access to that information.
- Ensure that personal information obtained and held is as accurate and complete as necessary for the purpose you use it for.
- Ensure the security of information and keep it only as long as reasonable for business or legal reasons.
- Designate a privacy officer to ensure your organization complies with PIPA regulations.
- Develop policies and procedures necessary for your organization to meet its PIPA obligations.
- Develop a complaint process respecting the application of PIPA, and make these available to individuals upon request.
- Make attempts to resolve complaints quickly and in good faith.

Despite PIPA, BC organizations that engage in commercial trans-border flows of information must follow PIPEDA regulations concerning this.

www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

Freedom of Information and Protection of Privacy Act (FOIPPA)
FOIPPA is British Columbia's Privacy legislation for public organizations such as government agencies, court records, colleges and universities established by provincial charter. It does not apply to churches.

The purpose of FOIPP is to make public bodies more accountable for the information they keep and to ensure members of the public have the right to information about themselves.

One aspect of FOIPP that confuses churches is that it prohibits public agencies (but not churches) from holding electronic information on servers or archives in another country such as the United States. This does not apply to churches, but does apply to colleges. Personal information that is subject to FOIPPA is excluded from B.C. PIPA legislation.

Manitoba, Saskatchewan, all Territories

Manitoba, Saskatchewan, Nunavut, Yukon and the Northwest Territories have no privacy legislation of their own, so the principles of federal legislation, PIPEDA, apply.

This means churches are not technically subject to the legislation because of the PIPEDA's focus on commercial activities. Churches should implement privacy policies as a Best Practice.

Privacy's Everyday Impact

Whether or not privacy legislation applies, it is a Best Practice for churches to develop and implement privacy policies and procedures.

General
Churches can develop privacy policies and procedures that comply with legislation in force in their jurisdiction. Information should be held securely and distributed only as appropriate on a need to know basis to maintain confidentiality.

Churches must appoint a Privacy Officer in BC and should appoint one in other provinces or territories.

Churches have a fiduciary duty to consider donor lists and contact information as charitable property and are restricted from sharing those lists.

Commercial Activities
Sharing, selling or bartering member lists is a commercial activity. This can be done only with prior permission from anyone and everyone on the list. Remember, all organizations that engage in commercial activities must comply with privacy legislation.

Running a daycare, school or business is considered a commercial activity and is subject to privacy laws. Fundraising is not considered a commercial activity, whether this is for huge capital projects or a church bake sale for the youth ministry. Sending out newsletters is not considered a commercial activity.

Privacy's Everyday Impact Continued

Information Collection
Churches are likely safer to obtain information from members on an "opt-in" basis where individuals intentionally give consent to have their information collected, used and distributed. Usually, it is good for congregants to opt in annually.

Keep information collection purposes general so they apply broadly and require information to be collected only once, such as for:

- Personal support
- Spiritual and social opportunities
- To verify identity
- For distribution of tax or expense receipts
- For inclusion in directories
- Enrolment in programs
- Inclusion in online databases

Directories

- Creating a directory is not considered commercial activity.
- Churches may have member directories that include personal contact information and photos.
- Directories should specify in writing that they are for private, internal use only and that they are not to be sold, lent or bartered, or to be used by congregants to pursue commercial activities.
- It is inadvisable to include minor children's names in directories.
- Directories should be considered as internal documents provided to members only rather than leaving them to be picked up in places accessible to non-members, such as the church foyer or website.
- It is safer to have congregants opt in to being listed in a directory rather than having them opt out of being included automatically. By opting in, congregants have more choice and control over their own information.
- Everyone listed in a directory should be asked to review their information annually for accuracy and completeness.

Websites

- Churches may store personal information and databases on websites, computers, staff notebooks, sticky notes paper documents, whiteboards, blackboards, etc. provided the information is held with consent, is secure and accessible only for the intended uses and viewers, and is accessible to the individual it belongs to.
- Churches may store information and databases on servers in other countries like the United States.
- Websites should include a copy of the church's privacy policy.

Other Considerations

Emergencies
During an emergency situation, such as a fire, accident or child abduction, personal information (such as name, age, height, gender, health issues, address) may be given to the appropriate first responders without the consent of the individual.

Common Sense
Common sense, courtesy and pastoral responsibilities for confidentiality should cover most privacy issues related to pastoral care and normal church activities such as personal counselling, sharing prayer concerns, signing up for events.

Use common sense in faxing or emailing financial or sensitive information and do so only when necessary. A good rule of thumb is to email only information that you would feel comfortable sharing by phone.

Churches must treat the information of both staff and volunteers the same.

Reasonable Collection
Churches may not collect information not reasonable for its purposes, such as medical or financial information. If this information is necessary for the work of the church in relation to the individual it may be collected.

Board meetings are not considered private (unless in-camera) and may be made public, although not if they include personal information. Publication of board minutes on websites isn't advisable.

Photos of church members that identify the person can only be published with written, verbal or tacit consent.

Prayer concerns should be shared only with those from whom an individual has requested prayer such as a pastor, prayer circle or the deacons. Concerns, health information, employment status or personal issues should never be shared publicly without the consent of the individual.

Churches may keep archives or historical records that include personal information as long as the information is not considered too sensitive for disclosure, the person has been dead 20 years or the information has been in a record for more than 100 years.

It is helpful for churches to establish information access protocols defining who should have access to what type of personal information. For example, a treasurer may need to know about an individual's donations to provide a tax receipt but has no need to know about a person's prayer concerns.

Steps to Protect Privacy at Your Church

1. Assign a Privacy Officer or Team
Put someone (or a team) in charge who has responsibility to review all aspects of privacy in your church. To ensure accountability and 'corporate memory' it is often best to assign a staff person as Privacy Officer or at least to make a staff person part a member of a privacy team.

2. Get Educated
The Privacy Officer should learn about privacy legislation and share that knowledge with staff and congregants.

Don't assume rumours about the impacts of legislation are true. Find out.

3. Assess
Find out how your church deals with personal information. What information do you collect? Why? Do members know the information is being collected? Do they know why? How is information collected? Who has access to the information? How is it stored? How long is it kept? When is it destroyed? What happens if there is unauthorized access to information?

4. Compare
Compare your practices to the requirements of legislation.

Contact the CBWC's Privacy Officer Bill Mains, who is also available through the Vancouver office. Contact other churches to learn from them and share information.

5. Develop Privacy Policies and Practices
Privacy policies should cover:
- Type of information gathered
- Uses of information
- How you will ensure accuracy of information
- Storage and disposal of information
- Ways to gather information
- Ways to erase or delete information
- Security measures
- Staff's personal information about employment

Put all policies and procedures in writing. This provides easy, authoritative reference and ensures there is an "institutional memory" of policies and practices.

6. Train
Train staff in:
- the principles, policies and practices of your church.
- How their jobs are affected
- What to do if security is violated – how will you assess harm? Who will be notified, when, how and by whom?
- how information will be used
- your church's privacy policies and practices
- how individuals can access information about themselves
- where individuals can get more information about privacy legislation, policies and practices

7. Inform
Let your members know:
- what information is collected
- why information is collected

Add notices about privacy policies and practices, including purposes for the information collected to forms, documents, websites, publications etc.

8. Enforce
Update staff contracts and volunteer forms to clarify that the church is legally responsible to protect personal information and set out expectations about how individuals will collect, use or disclose information.

9. Update
- Keep your policies and procedures current by reviewing them annually.
- Annually review what information is collected, by who, how, and why.
- Regularly update information to add new information or delete old/unneeded information. For example, get congregants to verify and correct information in directories annually, and sign off on it.
- Annually review stored information for accuracy, purpose of storage and security.

If Personal Information is Wrongly Disclosed

Sometimes, privacy is breached accidentally (or intentionally). It can happen through lost notebooks, uncontrolled access to computer records, inappropriately shared prayer concerns, theft or in many other ways. In a complex organization like a church with many people who have access to information, it is almost inevitable. Here's what you can do if it happens:

Understand What Happened and Why

- Designate the Privacy Officer or team to investigate how the breach happened
- Find out what personal information was involved
- Find out how many people were impacted and whether other organizations were affected, such as other churches, employees, contractors, volunteers, service providers etc.
- Find out what form the information was in (electronic database, notebook, paper records, tax receipts, verbal information)
- When was privacy violated and how?
- How did the breach become known?
- Is it possible to determine who breached an individual's privacy?

Act Quickly to Minimize the Impact of the Privacy Breach

- Empower the Privacy Officer to contain the breach and minimize its impact.
- Contain the breach by recovering lost notebooks, changing locks, shutting down computers, changing passwords – depending on how access to information was gained
- Determine who needs to know about the breach, including the person(s) whose information was shared, and possibly police, lawyers, accountants etc.
- If the breach involves criminal activity, notify the police
- Ensure that evidence about the security breach is not destroyed

Evaluate the Risks Associated with the Breach

- Based on the information that was disclosed, determine the possible harmful outcomes that could result, such as to personal safety, physical harm, damage to reputation, humiliation, identity theft, financial losses etc.
- Determine the risk of future disclosure caused by the people who obtained the information
- Determine what harm there might be to your church because of the disclosure of information, such as lost of trust, financial losses, legal action etc.
- Determine whether the disclosure of information might harm the public in any way.
- Determine what physical or technical security measures were in place at the time of the breach (passwords, padlocks, alarms, data encryption etc.)
- Determine if there is a risk of further breaches
- Was the information lost or was it stolen? If stolen, was the information the intended target of the theft or an unintended outcome of the theft?
- Has the personal information been recovered?
- Is this a routine problem or an isolated incident?

Notify the People Affected by the Security Breach

- Determine who has been affected and should be notified
- Determine who else, apart from those affected, should be informed, such as credit card companies, financial institutions, insurance agencies, police, the CBWC, employees, volunteers etc.
- Determine who (i.e. Privacy Officer, Pastor, Moderator/Chair of church, lawyer) should communicate with the person(s) whose privacy was breached
- Determine what information will be communicated to those affected
  - when, how, why, what, who
  - what the church will do to help individuals to reduce the risk of harm to themselves
  - what steps the church has taken or is taking to remedy this situation to prevent future privacy lapses
  - contact information for future updates
- Ensure that notification is done as quickly as feasible, apart from delays necessary to avoid compromising criminal investigations
- Notify the individuals whose privacy has been violated
- If you feel there is no need to notify the individuals in the case of a very minor breach, note your reasons in a permanent record
- Understand your church's legal and contractual obligations

Prevent Future Breaches of Privacy

Take steps to minimize the chances of accidental disclosure or theft of private information by responding to the root causes of the incident, including:

- Updating privacy policies and procedures
- Training staff and volunteers about privacy and confidentiality Obtaining the physical or electronic security systems needed to safeguard records

Canadian Baptists
OF WESTERN CANADA