REPORT | THIRD SESSION | FORTIETH PARLIAMENT

Special Committee to Review the Personal Information Protection Act

LEGISLATIVE ASSEMBLY
PROVINCE OF BRITISH COLUMBIA

FEBRUARY 2015

February 6, 2015

To the Honourable
Legislative Assembly of the
Province of British Columbia

Honourable Members:

I have the honour to present herewith the Report of the Special Committee to Review the *Personal Information Protection Act*.

Respectfully submitted on behalf of the Committee,

Mike Bernier, MLA
Chair

Table of Contents

Composition of the Committee

Members

Mike Bernier, MLA	Chair	Peace River South
George Heyman, MLA	Deputy Chair	Vancouver-Fairview
Donna Barnett, MLA		Cariboo-Chilcotin
Dr. Doug Bing, MLA		Maple Ridge-Pitt Meadows
Simon Gibson, MLA		Abbotsford-Mission
Sue Hammell, MLA		Surrey-Green Timbers
Marvin Hunt, MLA		Surrey-Panorama
Doug Routley, MLA		Nanaimo-North Cowichan

Committee Staff

Kate Ryan-Lloyd, Deputy Clerk and Clerk of Committees

Susan Sourial, Committee Clerk

Helen Morrison, Committee Research Analyst

Byron Plant, Committee Research Analyst

Terms of Reference

On February 25, 2014 and October 9, 2014, the Legislative Assembly agreed that a Special Committee be appointed to review the *Personal Information Protection Act* in accordance with section 59 of the *Personal Information Protection Act* [SBC 2003, c. 63] and, in particular, without limiting the generality of the foregoing, the collection, use and disclosure of personal information by organizations.

The Special Committee shall submit a report arising out of the results of its inquiry to the Legislative Assembly within one year of this resolution being adopted by the House. The Special Committee shall have the powers of a Select Standing Committee and in addition is empowered:

a. to appoint of their number, one or more subcommittees and to refer to such subcommittees any of the matters referred to the committee;

b. to sit during a period in which the House is adjourned, during the recess after prorogation until the next following Session and during any sitting of the House;

c. to conduct consultations by any means the committee considers appropriate;

d. to adjourn from place to place as may be convenient; and

e. to retain such personnel as required to assist the committee;

and shall report to the House as soon as possible, or following any adjournment, or at the next following Session, as the case may be; to deposit the original of its reports with the Clerk of the Legislative Assembly during a period of adjournment and upon resumption of the sittings of the House, the Chair shall present all reports to the Legislative Assembly.

Executive Summary

The Special Committee to Review the *Personal Information Protection Act* was mandated by the Legislative Assembly on February 25, 2014 and October 9, 2014, to conduct a review of BC's private sector privacy legislation, the *Personal Information Protection Act* (PIPA), as required by section 59 of the Act.

PIPA requires organizations to protect the personal information in their custody or under their control and governs how they collect, use, and disclose personal information. It also gives individuals a right to access and request correction of their personal information. The Information and Privacy Commissioner for British Columbia, an independent officer of the Legislative Assembly, is responsible for monitoring how PIPA is administered to ensure that its purposes are achieved. Because of the importance of privacy laws, PIPA requires a comprehensive review of the Act by a special committee of the Legislative Assembly at least once every six years. The first statutory review was undertaken by a special committee during 2007-2008, culminating in its Report in April 2008.

After organizational and planning meetings, the Committee commenced its review with technical briefings from the Ministry of Technology, Innovation and Citizens' Services and the Information and Privacy Commissioner and her staff. The Committee consulted with stakeholders and interested British Columbians over the following months. A public call for written submissions was advertised, inviting stakeholder groups and citizens to provide input on PIPA's provisions. Over the course of the consultation period, the Committee heard support for the overall approach and general principles of the Act as well as proposals to amend specific parts of the Act in order to address new issues or technical concerns. Following the public consultations, the Committee received additional technical briefings from the Ministry and the Information and Privacy Commissioner, and then undertook deliberations with respect to conclusions and recommendations.

The Committee concluded by reiterating a key finding of the 2007-2008 review, that the general approach and principles of PIPA are effectively serving the privacy interests of British Columbians. The Committee recommended changes in specific areas which would update statutory provisions and strengthen privacy protection for citizens, including measures to enhance accountability, the collection, use and disclosure of information, responsibility for personal information after transmittal, and access rights; improve the oversight authority of the Information and Privacy Commissioner; and respond to recent court decisions. In addition, the Committee recommended that the provincial government develop a new health information privacy law. Given that to date the 2008 recommendations have not been implemented, the Committee recommended that the provincial government report publicly on its response to the Committee's recommendations and its implementation plans in a timely manner.

The Statutory Framework

British Columbians live in an increasingly digital world, where technology contributes to the success of all sectors of the economy, and to the prosperity of communities and families. Supporting and balancing the evolving interests of the new economy and private citizens is an ongoing challenge for public policy discussions by British Columbians, their government, and their elected representatives.

In 2000, federal private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), was adopted, regulating the way Canadian businesses collect, use and disclose the personal information of their customers. PIPEDA applies in all Canadian provinces, unless a province has enacted a "substantially similar" privacy law.

In 2003, the Legislative Assembly of British Columbia adopted the *Personal Information Protection Act* (PIPA), drawing on the 2001 recommendations of an all-party Special Committee on Information Privacy in the Private Sector, which highlighted the need for information privacy legislation for BC's private sector, and for harmonization with federal law. The Act came into force on January 1, 2004.

To reflect the importance of privacy laws for all British Columbians, PIPA included a provision (section 59) which establishes a regular statutory review process by an all-party special committee of the Legislative Assembly – within three years of the coming into force of the Act, and at least once every six years thereafter.

The purpose of PIPA is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. There are over 380,000 organizations within British Columbia that are subject to PIPA. The spectrum includes businesses, credit unions, insurers, law firms, physicians' offices, unions, strata councils, non-profits, and political parties.

A statutory officer of the Legislature, the Information and Privacy Commissioner for British Columbia, provides ongoing accountability for the administration of PIPA. The Commissioner is responsible for monitoring how PIPA is administered to ensure that its purposes are achieved. Among other things, the Commissioner may initiate investigations or audits to ensure compliance. The Commissioner has the power to order organizations to respond to requests.

PIPA is distinct from BC's public sector privacy law, the *Freedom of Information and Protection of Privacy Act* (FIPPA), which governs how public bodies collect, use and disclose personal information, and confers public access rights to information in the custody or control of public bodies.

Only Quebec, Alberta and British Columbia have enacted private sector privacy laws that are substantially similar to PIPEDA. As a result, PIPEDA applies to the private sector in other provinces

as well as to federally-regulated works, undertakings and businesses such as banks, telecommunication companies, airlines and railways throughout the country.

PIPA is a consent-based statute, which means that, generally, organizations must obtain the consent of individuals to collect, use and disclose their personal information (there are a number of exceptions, including in relation to employee personal information which may be collected, used and disclosed without consent). An individual may be deemed to consent if the purpose for the collection, use or disclosure would be considered to be obvious to a reasonable person and the individual voluntarily provides the personal information for that purpose. An individual may withdraw consent. An organization must protect personal information in its custody or under its control by making reasonable security arrangements and must destroy personal information when retention is no longer necessary.

Within government, the Ministry of Technology, Innovation and Citizens' Services is responsible for the policies and administration of PIPA.

Legislative History

Minor amendments were made to PIPA following its adoption in 2003.

- *March 23, 2004*: The *Business Practices and Consumer Protection Act* (SBC 2004, c. 2), included consequential amendments to two definitions (effective July 4, 2004).
- *October 21, 2004*: The *Miscellaneous Statutes Amendment Act* (No. 3) (SBC 2004, c. 67) included amendments to correct erroneous or ambiguous wording and to allow the Information and Privacy Commissioner to share information with federal and provincial counterparts to help coordinate cross-jurisdictional privacy investigations.
- *May 18, 2006:* The *Miscellaneous Statutes Amendment Act (No. 2)* (SBC 2006, c. 24) included amendments to permit the collection, use and disclosure of third-party personal information without the consent of the third party when the information is necessary to provide services such as medical counselling or legal services to an individual who is the source of the third-party information. Additional amendments provided for a lawyer to refuse access to personal information where the file is subject to a solicitor's lien for non-payment of legal fees.
- *March 15, 2007*: The *Public Inquiry Act* (SBC 2007, c. 9) included consequential amendments to the powers of the Commissioner in conducting investigations, audits or inquiries (effective June 21, 2007).
- *May 16, 2007*: The *Attorney General Statutes Amendment Act, 2007* (SBC 2007, c. 14) included minor amendments (effective December 1, 2007).

The 2007-2008 Statutory Review

The first statutory review of PIPA was conducted by an all-party special committee in 2007-2008. After a public consultations process and deliberations by Committee Members, the Committee's report was presented to the Legislative Assembly in 2008, with 31 recommendations.

The 2008 Committee's recommendations proposed a range of statutory amendments, notably changes to enhance accountability for cross-border data flows, require mandatory notification of privacy breaches in certain circumstances, ban the use of blanket consent forms by provincially regulated financial institutions, revise consent exceptions to better address business practices in the insurance industry, permit disclosure of personal contact information for health research, retain the minimal fee for access to personal information, streamline the complaints process in the province's privacy laws, and strengthen the Information and Privacy Commissioner's oversight powers.

To date, none of the 2008 recommendations have been implemented. During this review, the Committee was advised by the Ministry of Technology, Innovation and Citizens' Services that as a result of the Ministry's own review and consultations, the Ministry has "agreed to propose amendments to PIPA based on those 2008 recommendations at the next available opportunity." The Committee is concerned that despite this, there has been a significant delay in proposed amendments being introduced in the Legislative Assembly.

In the years since the 2008 report was presented, some of its recommendations have been overtaken by events or are no longer appropriately worded. As a result, a new statutory review provides an opportunity to revisit and update the 2008 recommendations.

The Work of the Committee

On February 25, 2014 and October 9, 2014, the Legislative Assembly appointed the Special Committee to Review the *Personal Information Protection Act* to conduct the second statutory review of PIPA, including the collection, use and disclosure of personal information by organizations.

Planning and Organization

The Committee met on March 11, 2014 to plan and organize its work, and on May 14, 2014 to approve a business plan for its work, including a workplan for technical briefings, public consultations, and preparation of a report to the Legislative Assembly summarizing the results of the public consultations and providing the Committee's recommendations.

Technical Briefings

The Committee received initial technical briefings on May 14, 2014 from senior officials of the Ministry of Technology, Innovation and Citizens' Services and on May 28, 2014 from the Office of the Information and Privacy Commissioner.

Ministry officials discussed the historical beginnings of private sector privacy legislation in guidelines of the Organisation for Economic Co-operation and Development and a model code of the Canadian Standards Association. The Ministry explained that PIPA was first enacted because businesses at the federal level were finding PIPEDA complex and difficult to interpret and it was felt that the regulatory framework had to be workable and easy to apply for small businesses in the provincial setting. There was strong stakeholder support for provincial private sector privacy legislation at the time.

The Ministry indicated that support for PIPA remains high and that the Act is working well. The Ministry went on to explain the scope of application of PIPA and the definition of "personal information." The Ministry also briefed the Committee on fair information practices.

The Ministry informed the Committee of government's response to recommendations to amend PIPA that were made in the 2008 Report of the first Special Committee to Review the *Personal Information Protection Act*. The Ministry advised that the recommendations that were made "have been worked on by government, and all have been accepted. There are proposals that these would be put forward as possible amendments." The Ministry identified proposed amendments to PIPEDA and a 2013 Supreme Court of Canada decision as recent key developments.

The Information and Privacy Commissioner spoke to the impact of information technology on the collection, use and disclosure of information and on privacy protection. The Commissioner explained how her office exercises its oversight role in relation to PIPA, including complaint resolution, enforcement powers, providing education and advice, collaboration with the Alberta and federal

offices, and involvement in the Global Privacy Enforcement Network and the Asia Pacific Privacy Authorities. In her written submission, four major PIPA reform considerations were outlined: mandatory breach notification; order-making power on a Commissioner-initiated investigation; warrantless disclosures; and the 2013 Supreme Court of Canada decision.

The Ministry and the Information and Privacy Commissioner appeared before the Committee again on November 26, 2014 after the Committee's public consultation process was completed.

Ministry officials discussed mandatory breach notification and recent Supreme Court of Canada rulings. The Ministry also commented on other submissions received by the Committee, including concerns that were raised with respect to the *Strata Property Act*, and advised the Committee of training opportunities it provides to organizations. The Ministry reiterated that overall PIPA continues to work well, but noted that as with any legislation, updates and clarifications are always necessary.

In her presentation, the Information and Privacy Commissioner submitted that PIPA is a balanced and effective law that is very current, but that in light of new technological developments and court decisions it needs to be updated. The Commissioner saw the need for additional accountability provisions in relation to privacy management programs, mandatory breach notification, and transmittal to third parties as well as limits to warrantless disclosures to law enforcement. The eleven specific recommendations of the Information and Privacy Commissioner detailed in her written submission are discussed in the Committee's consideration of the public consultation results and recommendations.

Following the public hearings, the Committee sought further input and clarification from the Information and Privacy Commissioner on specific recommendations that it had received. The Commissioner responded to the Committee's questions in letters dated January 12 and 27, 2015. In a couple of instances, she undertook to revise guidelines or issue new ones to ensure that concerns are addressed.

Consultation Methods

The Committee established a range of methods to meet its mandate and collect public input on PIPA and the collection, use and disclosure of personal information by organizations.

A province-wide news release was issued on June 24, 2014, announcing that the Committee was conducting a review of PIPA and inviting the public to make submissions by September 19, 2014. A Committee webpage was launched, with information on how to participate in the public consultations. Advertisements were also placed in major newspapers, inviting the public to contribute to the Committee's work. Invitations to participate in the Committee's public consultations were sent to stakeholders, including 200 associations and organizations.

On September 19, 2014, a second province-wide news release was issued extending the deadline to make a submission to October 24, 2014, to allow additional time for input. Public input was accepted via a web-based submission form, as well as by email, fax, and regular mail.

Public Hearing Presentations

A public hearing was held in Vancouver on September 8, 2014, to gather information from key stakeholders and interested individuals. Four organizations and one individual made presentations to the Committee: the BC Freedom of Information and Privacy Association; Central 1 Credit Union; OpenMedia; the Private Investigators' Association of BC; and Sandra Olson.

Written Submissions

The original deadline for receiving written submissions was June 24, 2014, which was subsequently extended to October 24, 2014. In total, 42 written submissions were received during the consultation period. The names of all individuals and organizations that made written submissions are listed in Appendix A.

Meeting Schedule

March 11, 2014	Organizational meeting
May 14, 2014	Approval of business plan Technical briefing
May 28, 2014	Technical briefing
September 8, 2014	Public hearing
October 10, 2014	Organizational meeting
November 26, 2014	Technical briefings
December 15, 2014	Deliberations
January 26, 2015	Deliberations
February 6, 2015	Deliberations Approval of report

The Committee thanks all those who participated in its work on the statutory review of PIPA. The Committee received numerous comments on privacy issues as well as proposals to improve the statutory framework, which have made important contributions to the Committee's deliberations and development of recommendations. The Committee also expresses its appreciation to the officials of the Ministry of Technology, Innovation and Citizens' Services and to the Commissioner and staff of the Office of the Information and Privacy Commissioner for their assistance and contributions in support of the Committee's review.

Developments Since the 2007-2008 Statutory Review

The Committee's technical briefings and public consultations provided background information on today's landscape and the changes which have occurred since the 2007-2008 statutory review. Privacy is an issue of growing importance for citizens across the province, given the expanding use of information by the private and public sectors and the increasing need to ensure the protection of personal information. New technologies are providing additional opportunities for the use of information as well as challenges in maintaining effective protection of information. Court decisions have affirmed the importance of privacy, and provided clarification on the application of privacy laws. Changes to federal legislation and global privacy rules can result in a need for amendments to provincial laws.

It is in the context of this rapidly evolving environment that the Committee conducted the second statutory review of PIPA.

The Growing Threat to Privacy

The Committee's public consultations demonstrated a growing threat to privacy as well as a greater awareness by British Columbians about the importance of privacy, their privacy rights, and the obligations of organizations to protect their personal information.

In recent years, new information technologies have been developed and used by organizations to collect and store tremendous amounts of personal information in mega databases, or in the cloud, easily and cheaply. Through online activity, large quantities of information about individuals can be tracked and stored. This big data lends itself to new uses for data, such as advanced analytics. Looking forward, new technologies such as wearable computer devices and remote controlled aerial vehicles (drones) will collect information in novel ways that will accelerate challenges to privacy. Given this prodigious volume and velocity of data flows, there are increased risks, and more far-reaching consequences, of data breaches, including identity theft, fraud, and reputational harm.

Major data breaches in both the public sector and the private sector have helped to bring privacy concerns to the fore in public discourse. The widespread use of the Internet, particularly Facebook, provides regular awareness of privacy policies and privacy settings. With more public interest and awareness, there is increasing recognition of the need for up-to-date legal requirements to protect personal information in the custody or control of organizations and public bodies.

Recent Court Decisions

The importance of privacy is being affirmed by court decisions, which are shaping the development and application of privacy laws across Canada. In a 2013 decision (*Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*) balancing privacy and the right of freedom of expression, the Supreme Court of Canada characterized privacy rights as follows:

> The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy. As this Court has previously recognized, legislation which aims to protect control over personal information should be characterized as "quasi-constitutional" because of the fundamental role privacy plays in the preservation of a free and democratic society.

In that case, the court ruled that Alberta's *Personal Information Protection Act* violated the *Canadian Charter of Rights and Freedoms* right of freedom of expression by restricting the union's collection, use and disclosure of personal information for legitimate labour relations purposes.

In a 2014 decision (*R. v. Spencer*), the Supreme Court of Canada further affirmed the importance of privacy and ruled that the collection of subscriber information from an Internet Service Provider without a warrant, for the purpose of law enforcement, was contrary to the right of individuals under the *Charter* to be protected from unreasonable search and seizure. The Court found that individuals have a reasonable expectation of privacy with respect to their Internet usage. In considering privacy interests and informational privacy, the Court found that the concept of privacy as anonymity may, depending on the circumstances, be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure. The Court quoted from a decision of Mr. Justice Doherty of the Ontario Court of Appeal that "Personal privacy protects an individual's ability to function on a day-to-day basis within society while enjoying a degree of anonymity that is essential to the individual's personal growth and the flourishing of an open and democratic society."

Changes to Federal Legislation

In 2010, the federal government introduced changes to PIPEDA, which were reintroduced in 2014 as Bill S-4 (the Digital Privacy Act). The legislation reflects the federal government's view that PIPEDA provides a strong framework and that adjustments are needed to address new developments, notably in the areas of mandatory reporting of information breaches, revisions to the way business contact information is treated, and a threshold standard which would invalidate any consent obtained unless an individual can reasonably be expected to understand what they were consenting to. The federal government has expressed a commitment to advance the legislation, which may result in requirements for changes to PIPA.

Public Consultation Results and Recommendations

The Committee's public consultations from June to October 2014 gave experts, stakeholders and individual British Columbians an opportunity to provide input to the Committee's review of the effectiveness of PIPA's provisions.

Overall Approach and General Principles

The Committee received technical briefings and submissions, which provided evidence that PIPA's overall approach and general principles are working well, that a coordinated approach with Alberta and federal legislation is desirable, and that adjustments to statutory provisions would enhance the effectiveness of the Act by addressing new challenges.

Committee Members affirmed the conclusion of the 2007-2008 statutory review respecting PIPA's importance in providing a comprehensive, principles-based approach to the protection of personal information in the custody or control of organizations. They also supported the value of a statutory review process in engaging the Members of the Legislative Assembly in this key area of concern to British Columbians, and in providing citizens with a regular forum for expressing their views on the effectiveness of PIPA's provisions to their elected officials.

Members expressed their support for the 2008 Report and recommendations of the previous Committee, subject to minor modifications in the wording of the 2008 recommendations in relation to mandatory breach notification, consent requirement for the collection of witness statements, and who may act for deceased persons which are explained later in this report. Based on information from the Information and Privacy Commissioner, the Committee adjusted a 2008 recommendation on a requirement to make written privacy policies publicly available; and on fees for access. The Committee also modified a 2008 recommendation on disclosure to a law enforcement agency to reflect the implications of a recent Supreme Court of Canada decision. With respect to two recommendations that were made to the Information and Privacy Commissioner, the Commissioner advised that one had been implemented but that one was not because the matter was no longer an issue.

Accountability

Privacy Management Programs

PIPA states that an organization is responsible for personal information under its control, including information that is not in its custody [section 4(2)]). It also requires organizations to:

- designate one or more individuals to be responsible for ensuring that the organization complies with PIPA [section 4(3)];

- develop and follow policies and practices that are necessary for the organization to meet the obligations of the organization under PIPA [section 5(a)];
- develop a process to respond to complaints that may arise respecting the application of PIPA [section 5(b)];
- make information available on request about policies and practices and the complaint process [section 5(c)]; and
- make reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks (section 34).

In her final submission to the Committee, the Information and Privacy Commissioner advised that these are accountability requirements and that there is an emphasis, globally, in promoting accountability for privacy. For example, the Organisation for Economic Co-operation and Development recently revised its guidelines to add new sections addressing accountability.

The Information and Privacy Commissioner stated that in the context of PIPA, "accountability is an organization accepting and being able to demonstrate responsibility for personal information under its control." The Commissioner proposed that PIPA be amended to require organizations to build accountability into their operations by adopting privacy management programs that:

- are tailored to the structure, scale, volume, and sensitivity of the operations of the organization;
- make the privacy policies of the organization publicly available;
- include employee training;
- are regularly monitored and updated; and
- encompass existing obligations under PIPA.

The Commissioner also stated that organizations should be required to demonstrate a privacy management program to her Office upon request.

Committee Members expressed concerns about the impact that additional requirements would have on smaller organizations, particularly non-profit organizations, and that further legal obligations could be onerous. The Committee concluded that additional accountability requirements should be as simple as possible and should be flexible and scalable to what is sufficient and appropriate for the nature and size of the organization and the amount and sensitivity of the personal information that it has under its control.

The Committee urges the Commissioner to continue her efforts to provide guidance and useful tools targeted to smaller organizations that are reviewed periodically. In particular, Committee Members stressed the need for web-based, easily accessible and graphically appealing guidance documents that

would provide detailed information to smaller organizations, including non-profits, about how to implement privacy management programs that meet PIPA requirements.

The Committee noted that the previous Committee, in its 2008 Report, recommended that no amendment be made to PIPA requiring an organization to make written privacy policies publicly available in view of a concern that the then–Information and Privacy Commissioner had expressed about the impact such a requirement may have on smaller organizations. However, the Committee was satisfied that given that the requirement would be scalable, it was unlikely that it would be problematic.

The Committee agreed that accountability is of critical importance to the effective implementation of PIPA and therefore recommends that:

Recommendation

1. PIPA be amended to require organizations to adopt privacy management programs that:
   - are tailored to the structure, scale, volume, and sensitivity of the operations of the organization;
   - make the privacy policies of the organization publicly available;
   - include employee training; and
   - are regularly monitored and updated.

Mandatory Breach Notification

A privacy breach is generally understood to be a loss of or unauthorized access or disclosure of personal information resulting from a breach of an organization's security safeguards.

A number of associations and the Information and Privacy Commissioner advocated a statutory requirement for organizations to notify the Commissioner and affected individuals in the event of a privacy breach. The Commissioner submitted that, "Mandatory breach notification would motivate greater compliance with PIPA, build awareness of obligations and help to ensure organizations take proactive measures to protect consumer data." In the words of the Privacy Commissioner of Canada, mandatory breach notification would "benefit the citizens of British Columbia by enhancing accountability and transparency, and helping to mitigate the fallouts of a privacy breach." Notification of affected individuals would give them the opportunity to protect themselves from risks such as identity theft and fraud.

Another rationale included harmonization with Alberta and with proposed amendments to federal legislation that are currently before Parliament. As stated by the Commissioner in her May 28, 2014 technical briefing: "Given that many businesses operate nationally or even internationally, it's confusing and it's difficult for businesses to have to comply with different requirements depending on whether they're federally regulated or provincially regulated or in what province the service is that

they provide. Harmonized laws will facilitate the understanding of organizations about their legal obligations, and harmonization promotes better compliance."

Support for mandatory breach notification was not universal, however. The Canadian Bar Association (BC Branch) Freedom of Information and Privacy Law Section was divided as to the need for mandatory breach notification, although it noted a sense of inevitability.

In its 2008 report, the first Special Committee to Review the *Personal Information Protection Act* recommended that mandatory breach notification be added to PIPA. Since then, mandatory breach notification has been implemented in Alberta and is included in proposed amendments to PIPEDA. Mandatory breach notification would ensure that PIPA maintains its designation as substantially similar to federal legislation, if the federal government's proposed amendments currently before Parliament are enacted.

The mandatory breach notification provision in the Alberta legislation reads as follows:

> 34.1(1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

The Alberta Commissioner has the authority to require organizations to notify individuals affected by a reportable breach and organizations are not prohibited or restricted from notifying individuals on their own initiative.

Proposed amendments to PIPEDA would require organizations to notify both the Privacy Commissioner of Canada and individuals about the breach.

> 10.1(1) An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.
>
> (3) Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

In terms of who should be notified, the previous Committee had recommended that organizations should be required to notify both affected individuals and the Office of the Information and Privacy Commissioner with a possible added requirement to notify credit reporting agencies or law enforcement agencies in cases where financial loss is a risk. However, given the desirability of harmonization with the Alberta and federal models, the Committee felt that organizations should only be required to notify affected individuals and the Commissioner.

Regarding a threshold for notification, the Canadian Bankers Association stated that only material breaches should be reported to the Commissioner. The Canadian Medical Protective Association stated that any breach notification provision should recognize there may be situations where notification is not required, such as where a breach is unlikely to result in harm or notification may actually give rise to a risk of harm. Harmonization with the threshold in Alberta was recommended by the Canadian Life and Health Insurance Association and the BC Civil Liberties Association. This was also the view of the Information and Privacy Commissioner who stated that it should be the same as the Alberta and proposed federal threshold – where there is a real risk of significant harm.

The Freedom of Information and Privacy Association suggested that organizations be required to notify individuals in all situations where a real risk of identity theft is created and that all breaches involving defined personal information should have to be reported to the Information and Privacy Commissioner. Committee Members noted that the 2008 Committee recommendation with respect to a threshold was that the kinds of personal information that must be involved before notice may be required should be considered, with personal information that is likely to create risks of financial loss or fraud and unauthorized disclosure of sensitive health information being key considerations. This greater specificity regarding risk based on the kinds of personal information involved may, however, be less desirable than simply stating any real risk of significant harm, since the nature of the risks are difficult to predict.

In her submission, the Commissioner noted the need to strike the right balance so as to avoid both "breach notification fatigue" (whereby consumers would start to ignore notification) and unnecessary obligations to notify where it would not be productive. The Special Committee accepts the recommendation of the Information and Privacy Commissioner that the threshold should be where there is a real risk of significant harm. It achieves the right balance in the appropriate level of risk to trigger notification requirements and is in harmony with the Alberta and proposed federal models.

The Commissioner recommended a number of other aspects of notification, including timing (without unreasonable delay), form and contents (to be prescribed) and penalties for failure to notify. The Commissioner seeks additional powers to order notification of individuals and to conduct investigations and audits of breach notification and security arrangement practices. Furthermore, the Commissioner submits that organizations should have a duty to document breaches, retain that information for at least two years and provide it to the Commissioner upon request. The Freedom of Information and Privacy Association and BC Civil Liberties Association also made recommendations regarding particulars of notification, including timing (within five business days), form and content of the notice, and mode of notification.

The Committee recommends that:

Recommendation
2. PIPA be amended to require organizations to notify both the Information and Privacy Commissioner and affected individuals of the loss of or unauthorized access or disclosure of personal information resulting from the breach of an organization's security safeguards where there is a real risk of significant harm.

Collection, Use and Disclosure

Collection Without Consent (Sections 12, 15 and 18)

As previously mentioned, PIPA is a consent-based statute, which means that generally, organizations must obtain the consent of individuals to collect, use and disclose their personal information, but there are certain limited exceptions. The Committee received a recommendation for another specific exception that would permit collection without consent.

The Insurance Bureau of Canada put forward a recommendation that PIPA should provide that "an organization may, during the course of investigating and settling contractual issues or claims for loss or damages under an insurance policy, collect, use and disclose a witness statement without the subject's knowledge or consent." This would permit insurers to collect, use and disclose witness statements in relation to contractual issues or insurance claims.

This recommendation was previously made by the Insurance Bureau during the 2007-2008 review. At that time, the Committee supported the recommendation after the development of a consensus between the Insurance Bureau of Canada and the then-Information and Privacy Commissioner.

In the view of the Information and Privacy Commissioner, PIPA should be amended to authorize the collection, use and disclosure of witness statements, but not of personal information generally as was recommended by the previous Committee in 2008. The Commissioner also did not support collection without consent for the purpose of settling contractual issues because this should be addressed in the terms of the contract. Committee Members concurred, noting that proposed changes to federal legislation would provide authority to collect, use and disclose, without the knowledge or consent of an individual, personal information that is contained in a witness statement related to an insurance claim. Therefore, the Committee recommends that:

Recommendation
3. a clause be added to sections 12, 15, and 18 to allow the collection, use, and disclosure without consent of personal information contained in a witness statement that is necessary for an insurer to assess, adjust, settle or litigate a claim under an insurance policy.

Disclosure Without Consent [Section 18(1)(k)]

Section 18(1)(k) of PIPA authorizes an organization to disclose personal information without consent "if there are reasonable grounds to believe that compelling circumstances exist that affect the health or safety of any individual and if notice of disclosure is mailed to the last known address of the individual to whom the personal information relates."

The Committee received a submission from the Ending Violence Association proposing that PIPA specifically authorize the collection, use and disclosure of risk related-information for the purpose of reducing the risk that someone will be a victim of domestic violence. Such an amendment would be consistent with a 2011 amendment to FIPPA that authorized collection and disclosure without consent if "the information is necessary for the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur."

In response to an enquiry by the Committee, the Information and Privacy Commissioner stated that specific authority to disclose information in a situation of domestic violence is not necessary given that section 18(1)(k) of PIPA already permits disclosure without consent in compelling circumstances that affect the health or safety of any individual. However, she indicated that the notice requirement, whereby a notice of disclosure must be mailed to the last known address of the individual, can be problematic in the context of domestic violence. To address that, she supported a limited exception to the requirement for consent in this instance.

The Committee agreed that there should not be a notice requirement when information about an individual is disclosed because of a risk of domestic violence and that PIPA should align with FIPPA in this respect. Therefore, the Committee recommends that:

Recommendation

4. PIPA be amended to remove the notice requirement in relation to the collection and disclosure of personal information without consent if the information is necessary for the purpose of reducing the risk that an individual will be a victim of domestic violence.

Access Rights

Fees for Access [Section 32(2)]

PIPA gives residents of British Columbia the right to access their personal information in the custody or under the control of private sector organizations. Pursuant to section 32(2) of PIPA, organizations may charge an individual who makes a request for access to their own personal information a minimal fee. Central 1 Credit Union and the Insurance Bureau of Canada submitted that organizations should be permitted to charge a reasonable fee rather than a minimal fee.

In the view of Central 1 Credit Union, a minimal fee is vague and does not acknowledge that it can be costly to carry out access requests, and that sometimes one request requires numerous detailed

searches. Similarly, the Insurance Bureau of Canada submitted that a minimal fee is unreasonable in the context of an insurance claims file where the insurer must collect personal information in order to investigate and settle the claim. In its view, an insurer should be able to charge a reasonable fee that accurately reflects the amount of time and effort that must be expended to properly process the access request.

The Information and Privacy Commissioner advised the Committee that her position remains the same as that of her predecessor during the 2007-2008 review. The then-Commissioner supported permitting organizations to charge a reasonable fee because of the inconsistency in PIPA on the issue of fees. PIPA permits an organization to charge a minimal fee, yet gives the Commissioner the authority to investigate whether a fee is reasonable. The former Commissioner noted that Alberta legislation permits the charging of a reasonable fee.

Committee Members noted that this recommendation was not supported by the 2008 Committee because a "minimal fee" acknowledged the entitlement that a person has to that information and that the reasonableness test in terms of the Commissioner's oversight is appropriate. However, the Committee considered that on balance "reasonable" would be an appropriate amount. It may differ according to the circumstance of the individual requesting the information as well as the size of the organization and the amount of work needed to fulfill the request. The Committee also supported the recommendation in the interests of internal consistency within PIPA and harmonization with Alberta legislation. Therefore, the Committee recommends that:

Recommendation
5. section 32 of PIPA be amended to permit organizations to charge a reasonable, rather than minimal, fee in relation to their responses to access requests.

Discretion Not to Respond to a Request for Access or Correction

Section 37 of PIPA permits organizations to request authorization from the Information and Privacy Commissioner to disregard an access request if the request would unreasonably interfere with the operations of the organization because of the repetitious or systematic nature of the requests, or is frivolous or vexatious.

In its submission to the Committee, the Insurance Bureau of Canada recommended that organizations should also be permitted to disregard requests that would either "amount to an abuse of the right to make those requests" (as in Alberta) or disregard requests that "are not consistent with the object of this Act" (as in Quebec).

The Committee was advised by the Information and Privacy Commissioner that the current wording of section 37 would authorize an organization to disregard requests when it would amount to an abuse of the right to make those requests or are not consistent with the purpose of PIPA. However, the Commissioner did not oppose an amendment, as it would further align PIPA with Alberta legislation, which contains similar wording.

The Committee recommends that:

Recommendation
6. section 37 of PIPA be amended to permit organizations to disregard access requests when it would amount to an abuse of the right to make those requests.

Responsibility for Personal Information after Transmittal

A schedule to PIPEDA contains a provision that expressly states that organizations are responsible for personal information they have transferred to a third party for processing. It reads as follows:

> Schedule 1 Principles set out in the National Standard of Canada entitled *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96
>
> 4.3.1 An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

Central 1 Credit Union and the Information and Privacy Commissioner submitted that PIPA should be consistent with federal legislation and expressly state that organizations retain responsibility for personal information they transfer to third parties for processing. The Alma Mater Society of UBC Vancouver also suggested that an addition to the Act could be useful on the issue of storing data outside the country.

The Information and Privacy Commissioner submitted that such a provision is needed in PIPA because of the extensive growth in the use of cloud computing by organizations in BC and around the world. Because these third-party cloud-computing companies are often located in other countries, the Commissioner indicated that "it is imperative that PIPA explicitly state that organizations remain responsible for personal information they transfer to third parties for processing or for service provision." The Commissioner acknowledged that section 34 of PIPA already requires organizations to be responsible for any personal information they send to third parties for processing or storage but submits that it should be explicitly stated to avoid confusion among businesses. The Commissioner also submitted that PIPA, like PIPEDA, should require organizations to ensure that those third parties provide the same level of privacy protection required by PIPA, regardless of where those third parties are located. This could be accomplished through third-party vendor contracts or by other comparable means.

Committee Members recognized the value of further clarity in this area, and supported an amendment that would clearly state that organizations are responsible for the personal information they transfer to a third party for processing, or for providing services to or on behalf of the transferring organization. Moreover, a requirement that organizations use contractual or other means to ensure that third parties comply with the requirements or PIPA, or provide a comparable level of

privacy protection, seems to be a necessary corollary to ensure that organizations fulfil their statutory obligations.

The Committee noted that these recommendations were made previously in the 2008 Report in relation to cross-border data flows.

The Committee considered that both proposed amendments were important measures to ensure the personal information of British Columbians is properly protected by third party processers or service providers wherever they are located. The Committee therefore recommends that:

Recommendation

7. PIPA be amended to expressly provide that:
   a) organizations are responsible for the personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization; and
   b) organizations must use contractual or other means to ensure compliance with PIPA, or to provide a comparable level of protection, for personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization.

Destruction of Records

Section 35(2) of PIPA requires an organization to destroy its documents containing personal information as soon as it is reasonable to assume that the purpose for the collection is no longer being served by retention and retention is no longer necessary for legal or business purposes.

The Committee received submissions in relation to destruction, including a recommendation made by the National Association for Information Destruction – Canada that a definition of destruction be added to PIPA and a recommendation by Robin Bayley that organizations should have an obligation to destroy personal information on request.

The 2008 Report recommended that destruction not be defined in PIPA. The Information and Privacy Commissioner endorsed that recommendation and pointed out that the existing requirement to destroy personal information in section 35(2) is technology-neutral and can evolve as technologies of information destruction and reconstitution evolve. The Committee agreed that a definition of destruction is not necessary or desirable.

The Committee considered the recommendation that organizations should have an obligation to destroy personal information on request. In response to an enquiry from the Committee, the Information and Privacy Commissioner noted the careful balance between the privacy rights of individuals and the legitimate business interests of organizations that are reflected in PIPA. She proposed that as an alternative, the Commissioner could be authorized to order an organization to return or destroy personal information when it is used or retained in contravention of PIPA. This would expand the Commissioner's existing authority under section 52(3)(f) of PIPA to require an

organization to destroy personal information collected in contravention of PIPA by adding order-making power in relation to the destruction of records that are used or retained in contravention of PIPA.

The Committee considered that the existing obligations pertaining to destruction could be strengthened by providing the Information and Privacy Commissioner with order making power in relation to the unauthorized retention of records. Therefore, the Committee recommends that:

Recommendation
8. PIPA be amended to empower the Information and Privacy Commissioner to make an order that personal information be returned or destroyed when it is used or retained in contravention of PIPA.

Permit Prospective Administrators to Access Personal Information of a Deceased Person (PIPA Regulations, section 3)

Section 3 of the Regulations made pursuant to section 58 of PIPA, sets out who may exercise the rights of a deceased person under PIPA. Currently this section allows a personal representative or the nearest relative of a deceased person to exercise the rights the deceased person would have had to request personal information and consent to its release. The previous Committee recommended in its 2008 Report that section 3 of the Regulations be amended to allow the release of information concerning the deceased's estate in the case of intestacy when a request is made by a solicitor on behalf of a person intending to apply for a grant of letters of administration.

The British Columbia Law Institute asked the Committee to consider broadening section 3 to permit other individuals who also need to access information concerning the estate of a deceased person when no executor is appointed. Prospective administrators need to obtain information concerning the assets and liabilities of the deceased in order to apply to court to be appointed the administrator of the estate. Although a recent change to the Supreme Court Civil Rules (March 2014) allows a prospective administrator to obtain from the court an authorization to obtain estate information, it is not working as intended, since financial institutions now require even executors named in a will to provide an authorization. The British Columbia Law Institute recommended that section 3 of the Regulations permit the disclosure of information at the request of: an executor named in the will; an administrator of the deceased; a prospective administrator who has obtained an authorization under the Supreme Court Civil Rules; or a solicitor acting for a prospective administrator.

This recommendation would expand the 2008 recommendation to include an executor named in the will; an administrator of the deceased; and a prospective administrator who has obtained an authorization under the Supreme Court Civil Rules in addition to a solicitor acting for a prospective administrator. The Information and Privacy Commissioner advised that she supports this expansion because they are necessary to fully address the same problem that the previous Committee sought to address in 2008.

The Committee concluded that the 2008 recommendation should be expanded as recommended by the British Columbia Law Institute. Therefore, the Committee recommends that:

Recommendation
9. section 3 of the PIPA Regulations be amended to permit the release of information concerning the estate of a deceased person at the request of an executor; an administrator of the deceased; a prospective administrator who has obtained an authorization; and a solicitor acting for a prospective administrator.

Decisions of the Supreme Court of Canada

The Committee received evidence about two recent decisions of the Supreme Court of Canada, which upheld rights under the *Canadian Charter of Rights and Freedoms* in the context of privacy law. Although these decisions concerned privacy laws in other jurisdictions, they raise the same issues in relation to PIPA, and therefore necessitate consideration of whether PIPA should be amended to address them.

Warrantless Disclosures

As noted earlier in this Report, a 2014 decision by the Supreme Court of Canada (*R. v. Spencer*) held that the collection of subscriber information from an Internet Service Provider without a warrant, for the purpose of law enforcement, was contrary to the right of individuals under the *Canadian Charter of Rights and Freedoms* to be protected from unreasonable search and seizure.

The Committee received a number of submissions that identified certain implications of the decision for the provisions of PIPA that permit warrantless disclosure [sections 18(1)(c) and (j)], which state:

> 18(1) An organization may only disclose personal information about an individual without the consent of the individual, if …
>
> (c) it is reasonable to expect that the disclosure with the consent of the individual would compromise an investigation or proceeding and the disclosure is reasonable for purposes related to an investigation or proceeding …
>
> (j) the disclosure is to a public body or a law enforcement agency in Canada, concerning an offence under the laws of Canada or a province, to assist in an investigation, or in the making of a decision to undertake an investigation

The Committee received a recommendation from the Freedom of Information and Privacy Association that both sections be amended because the current wording is too broad, confusing, and may be unconstitutional following the Supreme Court of Canada ruling. It should be clarified that disclosure is permitted only if the requesting agency meets the requirement of evidence of lawful authority, such as a court order, production order or warrant.

The Information and Privacy Commissioner submitted that amendments should be made to narrow the circumstances in which organization to organization disclosures can happen without consent to circumstances where the disclosure is necessary for purposes related to an investigation or proceeding [section 18(1)(c)], and to limit authority for warrantless disclosures to those that are initiated by the organization [section 18(1)(j)]. She also stated that organizations should be required to document and publish transparency reports on disclosures made without consent.

OpenMedia recommended to the Committee that the broad language of section 18(1)(c) be narrowed, and that section 18(1)(j) be removed. The Canadian Bar Association (BC Branch), Freedom of Information and Privacy Law Section recommended that section 18(1)(j) be reviewed because it is confusing and overbroad and needs clarification regarding whether lawful authority is required and what the nature of such authority would be prior to disclosure without consent. It also stated that "any amendments should not interfere with legitimate police work or with administrative or regulatory investigations, or take away an organization's ability to report a crime or provide information to prevent imminent harm to the health or safety of an individual." Christian Deck spoke to a public policy imperative: "Warrantless disclosures, except in cases of legitimate and dire emergency, are wrong, contrary to our right to privacy, and undermine the strength of our democracy."

Expressing a contrary view, the Canadian Life and Health Insurance Association stated that the authority to disclose personal information without consent for purposes related to an investigation [section 18(1)(c)] should not be amended because it is an effective tool in fighting against fraudulent activities.

The Ministry of Technology, Innovation and Citizens' Services advised the Committee that it is reviewing the Supreme Court of Canada ruling and its possible implications for PIPA.

Committee Members indicated that the overall view of the submissions received supported a narrowing of sections 18(1)(c) and (j) of PIPA because of the implications of the Supreme Court of Canada decision and the possibility of a *Charter* challenge. This would adjust a 2008 recommendation of the previous committee not to amend section 18(1)(j), in order to account for the implications of the recent Supreme Court of Canada decision. The Committee noted that the Information and Privacy Commissioner has recommended a balanced approach, and it concluded that the amendments she is proposing should be given careful consideration by the Ministry of Technology, Innovation and Citizens' Services. The Committee also agreed that organizations should be required to document and publish transparency reports on disclosures made without consent.

The Committee recommends that:

Recommendation
10. sections 18(1)(c) and 18(1)(j) of PIPA be amended to address issues raised by the decision of the Supreme Court of Canada in *R. v. Spencer* in accordance with the approach recommended by the Information and Privacy Commissioner. Organizations should be required to document and publish transparency reports on disclosures made without consent.

Labour Relations Disputes

As noted earlier in this Report, the Supreme Court of Canada held that the Alberta *Personal Information Protection Act* was invalid because it infringed on a union's expressive right in the context of labour disputes (*Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*). By restricting the videotaping of persons crossing a picket line, it infringed on the union's freedom of expression under the *Charter*, insofar as it restricted the collection, use and disclosure of personal information for legitimate labour relations purposes. The Court suspended its decision for 12 months to allow the Alberta Government time to amend the legislation. This timeline was later extended to May 15, 2015.

The Committee received evidence proposing that given the similarities between BC and Alberta private sector privacy legislation, PIPA also be amended by May 15, 2015 in order to remain valid. The Ministry of Technology, Innovation and Citizens' Services noted that PIPA contains a provision that allows organizations to collect and disclose personal information gained through observation at public events so that a ruling in BC may be slightly different. However, in the Ministry's view, the provision is probably not broad enough to address the labour issue.

In December 2014, the Government of Alberta enacted amendments to the Alberta statute to remedy the infringement. The key provision reads as follows:

> 20.1(1) Subject to the regulations, a trade union may disclose personal information about an individual without the consent of the individual for the purpose of informing or persuading the public about a matter of significant public interest or importance relating to a labour relations dispute involving the trade union if
>
> a) the disclosure of the personal information is reasonably necessary for that purpose, and
>
> b) it is reasonable to disclose the personal information without consent for that purpose, taking into consideration all relevant circumstances, including the nature and sensitivity of the information.

This is a very narrow exception, and the Information and Privacy Commissioner proposed to the Committee that PIPA be amended in a manner similar to what is enacted Alberta. The Freedom of

Information and Privacy Association and the BC Civil Liberties Association supported the Commissioner's proposal. The Freedom of Information and Privacy Association gave the following explanation as to why a narrow exception is preferable:

> A broader exemption, for example, one related to "labour relations activities" would capture essentially all the activities of unions and thus render the protections provided by the law illusory.
>
> Nor is exempting unions altogether from the application of PIPA the right approach: that would simply altogether deny individuals the right to request access to and correction of, their personal information; would exempt unions from the duties to protect the security of the personal information they collect, limit the collection, use and disclosure of the information; and to provide notice of the purposes and comply with the other obligations imposed by the law.

The Committee was advised by the Ministry of Technology, Innovation and Citizens' Services that government recognized that PIPA would need an amendment and was monitoring the Alberta response to ensure a consistency of approach.

Committee Members affirmed the value of amendments to PIPA to authorize a narrow exception, consistent with the Alberta amendments, which would address the possible infringement of a union's right of freedom of expression.

The Committee recommends that:

Recommendation
11. PIPA be amended to remedy the possible infringement of a union's right of freedom of expression through a narrow exception consistent with the Alberta amendments.

Oversight Authority of the Commissioner

Order-making Power on a Commissioner-initiated Investigation

The Committee received a submission from the Information and Privacy Commissioner that PIPA should be amended to provide her with the ability to make an order requiring an organization to implement recommendations she has made as the result of an investigation that she initiated. This would be consistent with the order-making power of the Commissioner pursuant to FIPPA.

Committee Members thought that it made sense for the Commissioner to have the same authority under PIPA as exists under FIPPA. Accordingly, the Committee supported the proposal of the Information and Privacy Commissioner to add this authority to PIPA, in order to provide for statutory consistency and to strengthen the ability of the Commissioner to enforce the requirements of PIPA.

The Committee recommends that:

Recommendation
12. PIPA be amended to empower the Commissioner to make an order on a Commissioner-initiated investigation.

Other Issues

The Committee received a variety of submissions highlighting other privacy issues and proposing amendments to address concerns ranging from the application of PIPA to service providers funded by government, exceptions to disclosure, new technologies, and the need for certification requirements. Some recommendations were outside the purview of the Committee.

Of these issues, the Committee focused its deliberations on solicitor-client privilege, concerns regarding the *Strata Property Act*, and health information privacy law.

Solicitor-client Privilege

Section 38(5) of PIPA provides that a copy of any document required by the Commissioner under section 38 must be provided to the Commissioner "despite any privilege afforded by the law of evidence." The Committee received evidence from the Law Society of British Columbia that this provision is inconsistent with section 3(3) of PIPA, which provides that "nothing in this Act affects solicitor-client privilege." The Law Society submitted that the power of the Information and Privacy Commissioner to compel the production of a document despite solicitor-client privilege should be removed because it does not adequately and properly protect the public interest in the administration of justice. If a question of privilege is being raised in connection with a document, the matter should be dealt with by the Supreme Court.

The Committee was advised by the Commissioner that solicitor-client privilege is not affected by disclosure to her Office. Documents are not made public or put to any purpose other than verifying that this exemption has been properly applied. If the Commissioner makes an order deciding against the privilege, the order is directed to the organization claiming the privilege and is subject to judicial review.

This same issue was raised by the Law Society during the last statutory review. The previous Special Committee supported the position of the Commissioner's Office and recommended that no amendment be made.

Committee Members considered the submission from the Law Society of British Columbia and the Commissioner's position that solicitor-client privilege is not affected by disclosure to her office, since documents are not made public or used for any further purpose. The Committee did not feel that any changes are needed to the existing authority of the Commissioner to compel the production of

documents. In the Committee's view, this authority is necessary for the Commissioner's ability to exercise effective oversight over compliance with PIPA.

Interplay with the *Strata Property Act*

Section 35 of the *Strata Property Act* requires strata corporations to prepare certain records, including minutes and books of account. It also requires strata corporations to retain copies of those records as well as other documents, including correspondence sent or received by a strata corporation or council. Section 36 requires a strata corporation to provide copies of the records and documents referred to in section 35 to a strata owner.

The Committee received submissions from individuals as well as the Condominium Home Owners' Association and the Vancouver Island Strata Home Owners Association about the application of PIPA to strata corporations and how that impacts statutory obligations of strata corporations to disclose information.

In their submissions, several individuals complained that strata corporations and councils "hide behind" PIPA to avoid having to release documents as required by section 36. If the records and documents contain personal information, the strata corporations and councils refuse to release them on the basis that PIPA does not permit them to do so. The Vancouver Island Strata Owners Association and three individuals submitted that PIPA should specifically exclude sections 35 and 36 of the *Strata Property Act* from its application.

The basis for these concerns appears to be the misinterpretation or misuse of PIPA by strata corporations. While strata corporations are subject to PIPA, this does not mean that they can ignore their duty to disclose certain records and documents under the *Strata Property Act*. The Ministry of Technology, Innovation and Citizens' Services and the Information and Privacy Commissioner advised that the disclosure of these documents is authorized by law and is therefore permitted under PIPA.

The Office of the Information and Privacy Commissioner has issued guidance on this topic in the past. Given what appears to be a significant misunderstanding of the requirements of PIPA in relation to strata corporations and councils, further guidance seems to be necessary.

In response to questions from the Committee, the Information and Privacy Commissioner advised that her Office is revising its privacy guidelines for strata corporations and strata agents and intends to use those revised guidelines to educate, and clarify matters for strata owners, councils and property managers.

The Committee recommends that:

Recommendation
13. the Office of the Information and Privacy Commissioner issue new guidelines for strata owners, strata councils, and property managers as soon as possible that will clearly explain the interplay between the requirements of the *Strata Property Act* and the requirements of PIPA.

Health Information Privacy Law

The Committee received a submission from the Canadian Medical Protective Association that recommended, among other things, that government enact new stand-alone health information privacy law as exists in other jurisdictions in Canada. The Association said that it would provide an effective governance framework for the provincial electronic health record to ensure there is a balance between privacy and subsequent use of information through data analytics. A separate health information privacy statute would have implications regarding the scope of application of PIPA because PIPA applies to health professionals in private practice. It would also carve out the Ministry of Health and health authorities from the scope of FIPPA.

In response to Committee questions, the Information and Privacy Commissioner advised that she is in favour of health-specific privacy legislation in BC because the health sector is unique and requires special consideration. She advised that she had issued a special report advocating such legislation in April 2014.

The Committee was of the view that the provincial government should develop a stand-alone health information privacy law that would govern how personal health information is collected, used, disclosed, and protected within the integrated health sector.[1]

The Committee recommends that:

Recommendation
14. the provincial government develop a new health information privacy law that is consistent with laws in other jurisdictions in Canada.

[1] The Committee was pleased to learn on February 2, 2015 that the Ministry of Health is beginning work on creating a framework to establish clear and consistent rules for the use and protection of personal health information in the public and private sectors.

Implementation of the Committee's Recommendations

Members expressed serious concerns about the status of recommendations to amend PIPA that were made in the 2008 Report of the previous Special Committee to Review the *Personal Information Protection Act*. As previously discussed in this Report, they have not been implemented. The Committee felt strongly that its recommendations for amendments to PIPA need to be implemented in a timely manner.

The Committee recommends that:

Recommendation
15. the provincial government report publicly on its response to the Committee's recommendations and its implementation plans in a timely manner.

Summary of Recommendations

The Special Committee to Review the *Personal Information Protection Act* recommends to the Legislative Assembly that:

1. PIPA be amended to require organizations to adopt privacy management programs that:
    - are tailored to the structure, scale, volume, and sensitivity of the operations of the organization;
    - make the privacy policies of the organization publicly available;
    - include employee training; and
    - are regularly monitored and updated.

2. PIPA be amended to require organizations to notify both the Information and Privacy Commissioner and affected individuals of the loss of or unauthorized access or disclosure of personal information resulting from the breach of an organization's security safeguards where there is a real risk of significant harm;

3. a clause be added to sections 12, 15, and 18 to allow the collection, use, and disclosure without consent of personal information contained in a witness statement that is necessary for an insurer to assess, adjust, settle, or litigate a claim under an insurance policy;

4. PIPA be amended to remove the notice requirement in relation to the collection and disclosure of personal information without consent if the information is necessary for the purpose of reducing the risk that an individual will be a victim of domestic violence;

5. section 32 of PIPA be amended to permit organizations to charge a reasonable, rather than minimal, fee in relation to their responses to access requests;

6. section 37 of PIPA be amended to permit organizations to disregard access requests when it would amount to an abuse of the right to make those requests;

7. PIPA be amended to expressly provide that:

    a) organizations are responsible for the personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization; and

    b) organizations must use contractual or other means to ensure compliance with PIPA, or to provide a comparable level of protection, for personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization;

8. PIPA be amended to empower the Information and Privacy Commissioner to make an order that personal information be returned or destroyed when it is used or retained in contravention of PIPA;

9. section 3 of the PIPA Regulations be amended to permit the release of information concerning the estate of a deceased person at the request of an executor; an administrator of the deceased; a prospective administrator who has obtained an authorization; and a solicitor acting for a prospective administrator;

10. sections 18(1)(c) and 18(1)(j) of PIPA be amended to address issues raised by the decision of the Supreme Court of Canada in *R. v. Spencer* in accordance with the approach recommended by the Information and Privacy Commissioner. Organizations should be required to document and publish transparency reports on disclosures made without consent;

11. PIPA be amended to remedy the possible infringement of a union's right of freedom of expression through a narrow exception consistent with the Alberta amendments;

12. PIPA be amended to empower the Commissioner to make an order on a Commissioner-initiated investigation;

13. the Office of the Information and Privacy Commissioner issue new guidelines for strata owners, strata councils, and property managers as soon as possible that will clearly explain the interplay between the requirements of the *Strata Property Act* and the requirements of PIPA;

14. the provincial government develop a new health information privacy law that is consistent with laws in other jurisdictions in Canada; and

15. the provincial government report publicly on its response to the Committee's recommendations and its implementation plans in a timely manner.

Appendix A: Written Submissions

Eighteen written submissions were received from the following organizations:

Alma Mater Society of UBC Vancouver
British Columbia Civil Liberties Association
British Columbia Government Retired Employees Association
British Columbia Law Institute
Canadian Bankers Association
Canadian Bar Association (BC Branch)
Canadian Life and Health Insurance Association
Canadian Medical Protective Association
Canadian Union of Public Employees (BC Division)
Condominium Home Owners' Association
Ending Violence Association
Insurance Bureau of Canada
Kiwassa Neighbourhood House
Law Society of British Columbia
The McArthur Consulting Group
National Association for Information Destruction - Canada
Office of the Privacy Commissioner of Canada
Vancouver Island Strata Owners Association

Twenty-four written submissions were received from the following individuals:

Robin Bayley
Eric Bernal
Elaine Corner
Christian Deck
Patricia Emery
George Greenwood
Stephen Hales
Sean Jordan
Buddy Lee
Randy Lines
Sophie Loehrich
Donald McLeod
George McNutt
Elizabeth Menzies
Bill Nelson
Miriam Nelson
Joseph Parranto
Ron Prach
Barbara Reed
James Rodney
Mike and Sharyn Romaine
Ken Strang
Assefash Yirgaw
Peter Zouras

Additional Written Materials

Letter from Elizabeth Denham, Information and Privacy Commissioner dated June 3, 2014
Letter from Elizabeth Denham, Information and Privacy Commissioner dated January 12, 2015
Letter from Elizabeth Denham, Information and Privacy Commissioner dated January 27, 2015