Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

STATUTORY REVIEW OF THE PERSONAL INFORMATION PROTECTION ACT

SUBMISSION TO THE SPECIAL COMMITTEE TO REVIEW THE PERSONAL INFORMATION PROTECTION ACT

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

November 26, 2014

TABLE OF CONTENTS

PREFACE

The *Personal Information Protection Act* ("PIPA") is a balanced and effective law that protects the personal information of individuals while at the same time recognizes the right of organizations to collect, use and disclose such information.

This submission recommends that, in light of significant technological developments, carefully prescribed changes to PIPA are required to give expression to the core purpose of the legislation enacted in 2004.

Since PIPA's proclamation, we have witnessed a staggering escalation in the volume of personal information that organizations collect from British Columbians. Rapid changes in computing technology in particular have allowed information to be processed in ways that were unimaginable 10 years ago.

PIPA must address those developments if it is to remain relevant to British Columbians and remain true to its purpose.

What follows are changes that I believe are necessary to achieve this. Most of these recommendations can be captured under the heading of accountability. Where an organization experiences a privacy breach and the release of that information poses a reasonable risk of significant harm to an individual, the organization must be accountable. One way to ensure this is to make it mandatory for the organization to report that breach to the individual and to my Office. Additional changes are recommended to further strengthen accountability.

Portions of the submission deal with recent court decisions that have a direct bearing on the interpretation of PIPA. Other portions respond to submissions by civil society groups, industry associations and other stakeholders. Our views are offered in the hope of providing some assistance to the Committee as it undertakes its deliberations. On this latter point the Committee should know I will be writing directly to stakeholders and offering to meet with them to discuss their concerns. It is my desire to assist these organizations where they may face challenges complying with the legislation.

I would add one last thought on legislative context. In 2004, the federal Cabinet declared British Columbia's law to be substantially similar to the federal *Personal Information Protection and Electronic Documents Act*. Whatever the Committee decides to recommend, I respectfully submit that it bear in mind the outcome of Bill S-4 currently before the Parliament of Canada as well as the Alberta legislature's response

to the Supreme Court of Canada decision effecting the constitutionality of its *Personal Information Protection Act*, legislation very similar to ours. As this submission sets out, it also important that changes to PIPA aim for harmonization with other privacy legislation across Canada.

I will of course, answer any questions the Committee may have about this submission or assist in any way I can.

November 26, 2014

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

1.0 INTRODUCTION AND CONTEXT

When first enacted in 2004, the *Personal Information Protection Act* ("PIPA") was one of the leading pieces of privacy legislation in the world.

It is principles-based legislation based upon the 1980 Organisation for Economic Co-operation and Development ("OECD") Guidelines, which set out the basic principles for the protection of people's privacy. These principles include:

- a limitation on the collection and use of personal information;
- assurances around data quality;
- the specification of purposes for collection; and
- requirements for security safeguards, openness, and individual participation.

These principles are a key reason why our legislation remains relevant in spite of the tremendous changes in technology that we have seen since 2004 that affect how our personal information is managed by organizations.

However, no significant changes have been made to PIPA since its enactment. This review of PIPA by a Special Committee of the Legislative Assembly of British Columbia is therefore critical and opportune. Critical because since the last review was conducted in 2008, there have been fundamental technological changes that have enabled an exponential increase in the type and amount of personal information collected, used and disclosed by organizations in British Columbia. Technology has raised the privacy stakes to such a degree that the Office of the Information and Privacy Commissioner ("OIPC") no longer has all of the tools necessary to enforce the requirements of PIPA and to protect the personal privacy of British Columbians.

This review is also opportune given recent changes in the legal landscape. Two significant decisions of the Supreme Court of Canada within the last year have considered the application of the *Canadian Charter of Rights and Freedoms* ("Charter") to statutes similar to PIPA. South of the border, a landmark decision of the United States Supreme Court further informs the reach of privacy rights. Legislation before the Parliament of Canada (Bill S-4) proposes to amend the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), the federal private sector privacy law to which PIPA must remain substantially similar. Another federal Bill (Bill C-13) is intended to address cyber-bullying, but does so in a manner that raises privacy concerns. There has been significant public debate about both Bills.

Finally, the Supreme Court of Canada's decision in *R. v. Spencer* is informative in the Special Committee's review of PIPA.

Part 1 of our submission provides introduction and examines the context surrounding PIPA in Canada and the world, including developments affecting privacy. Part 2 provides my recommendations to the Special Committee for updating PIPA and finally in Part 3, I offer comments on many of the recommendations that organisations and individuals have made to the Special Committee.

➢ MAINTAINING SUBSTANTIAL SIMILARITY: LEGISLATIVE CHANGES AND COURT DECISIONS

British Columbia is one of only three provinces that have enacted provincial privacy legislation – the other two are Quebec and Alberta.[1] Because PIPA must be substantially similar to PIPEDA, legislators in B.C. need to be aware of amendments to PIPEDA. This includes changes made through federal legislative proposals, such as Bill S-4, and changes or interpretation made to PIPEDA required by significant court decisions, such as those that we have seen in the past year with *Spence*r and *Alberta (Information and Privacy Commissioner) v. United Foods and Commercial Workers, Local 401 ("UFCW")*.

➢ PRIVACY IMPLICATIONS OF NEW TECHNOLOGIES

PIPA applies to some 380,000 organizations that collect, use and disclose the personal information of British Columbians. Its importance is heightened by the increasing amount of personal information that is collected, used and disclosed by organizations in the digital age.

Technology has made it easy and inexpensive for organizations to collect and store personal information about their clients in large databases or in the cloud. This information is in turn being used to conduct big data analytics and to track and predict consumer behaviour.

Novel ways of collecting personal information have also flowed from new technologies – examples include video surveillance, social media, wearable computing devices, street level imaging, and unmanned aerial vehicles (UAVs or drones). Similarly, the networked nature of the emerging "Internet of Things" will present novel challenges for privacy. We can expect technology to accelerate the collection of more and more personal information in the years to come.

We have also seen the dramatic growth of organizations using cloud-based processing and storage for information, including personal information. Although storage of personal information in the cloud can provide cost savings and efficiencies, it can result

[1] Organizations in the Province of British Columbia Exemption Order SOR/2004-220, at: http://laws-lois.justice.gc.ca/eng/regulations/SOR-2004-220/page-1.html#h-1. Note that Manitoba has passed a provincial private sector privacy law, but it has not yet been proclaimed in force.

in insecure storage, or unauthorized access and disclosure. Personal information stored outside of Canada may also be subject to lawful access demands by foreign governments, without the individual's knowledge, consent or remedy. Organizations must be aware that even if they use a third-party cloud service provider located in another country, they remain responsible under PIPA for any personal information stored in the cloud. An organization cannot contract out of its PIPA obligations to safeguard personal information.

With ever more personal information stored in databases and in the cloud – including sensitive medical information, financial information, consumer profiles and purchasing history – comes a higher risk of privacy breaches of greater magnitude and with more damaging consequences. This increased risk underscores the importance of robust privacy laws and strong enforcement tools.

➢ A LOOK AT THE FUTURE OF ENFORCEMENT: CO-OPERATION AND ACCOUNTABILITY

The Office of the Information and Privacy Commissioner promotes compliance with PIPA primarily through:

- education, outreach and guidance;
- investigations and mediations; and
- orders that have the force of law.

We continually work to promote a greater understanding and awareness of the requirements of PIPA by both organizations and their customers. We promote compliance with privacy obligations through strategic outreach such as a comprehensive user-friendly website, speeches, conferences, partnerships and consultations.

My Office also cooperates with our counterparts in Ottawa, Alberta, and other jurisdictions to promote compliance.[2] Co-operation has become a necessary aspect of enforcement at a time where data generally – and personal information more specifically – is increasingly being transferred across borders. Where necessary we co-operate on investigations and consult organizations operating inter-provincially or internationally. This co-operation ensures a consistent approach to privacy enforcement for private sector actors that operate across multiple jurisdictions.

[2] The OIPC has had a Memorandum of Understanding in place on cooperation with the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner of Alberta since 2004. In addition, data protection authorities and privacy commissioners from around the world have recently recognized the importance of co-operation in enforcement in its Resolution on Cooperation and Enforcement at the 36th International Conference of Data Protection and Privacy Commissioners: http://www.privacyconference2014.org/media/16430/Resolution-International-cooperation.pdf.

The aim of these co-operative efforts is to increase the number of organizations in compliance with PIPA, particularly if these efforts are supported by legislated accountability measures. With the personal information of B.C. residents becoming part of the new currency for the digital economy, we must ensure organizations are able to demonstrate their compliance with PIPA and protect the personal information of British Columbians.

➢ *SPENCER*: CLARIFYING THE WARRANT REQUIREMENT FOR DISCLOSURES WITHOUT CONSENT

Under section 8 of the *Charter*, "everyone has the right to be secure against unreasonable search or seizure". Therefore, any search and seizure may be subject to a *Charter* challenge if an individual has a reasonable expectation of privacy in relation to the information collected by police. There have been a number of decisions by the Supreme Court of Canada in the last decade that interpret whether, in the totality of the circumstances, individuals have a reasonable expectation of privacy.[3] The most recent example, *Spencer*, is a landmark decision in terms of the nature of privacy itself and the application of privacy protection to new technologies.

The matter at issue in *Spencer* was a police request to an internet service provider for subscriber information for the purposes of a police investigation without obtaining a warrant. The Supreme Court highlighted the fundamental links between privacy and democracy when it stressed the need for "…a purposive approach to s. 8 that emphasizes the protection of privacy as a prerequisite to individual security, self-fulfillment and autonomy as well as to the maintenance of a thriving democratic society."[4]

In *Spencer* the Court found that there exists a reasonable expectation of privacy in internet subscriber information, and that a police request to an organization for a subscriber's identifying information in relation to otherwise anonymous internet activity engages a high level of informational privacy. As a result, it found that the subscriber information was obtained unconstitutionally.

Spencer has shifted the landscape of disclosures made to police or public bodies without the consent of the individual; law enforcement must now obtain a warrant prior to requesting such disclosures of personal information. The Special Committee should consider the role that privacy rights play towards a healthy and vibrant democracy in its deliberations on recommendations for amendments to PIPA.

---

[3] *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432; *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456; *R. v. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569; *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211.
[4] *R. v. Spencer*, 2014 SCC 43, at 15.

2.0 MAJOR PIPA REFORM CONSIDERATIONS

2.1 ACCOUNTABILITY

People working in privacy around the world are paying significant attention to accountability and the ways in which it can promote privacy in a manner that balances the interests of multiple stakeholders. What is accountability? In the context of PIPA, accountability is an organization accepting and being able to demonstrate responsibility for personal information under its control.

B.C. was a global leader in privacy and accountability when PIPA was first enacted. This was in part because sections 4 and 5 of the legislation set out general obligations for organizations to have policies and individuals responsible for ensuring compliance with PIPA. Leadership was also demonstrated because section 34 of PIPA places a general obligation on organizations to protect personal information by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, modification or other such risks.

Beginning in 2010, the Privacy Commissioners for Canada, Alberta, and British Columbia worked together to respond to a growing need from organizations to better understand *how* to build accountability into their operations. This resulted in the 2012 publication of "Getting Accountability Right with a Privacy Management Program", a guidance document that sets out the essential building blocks for bringing accountability and privacy into practice in an organization.

The response to these guidelines has been overwhelmingly positive from organizations in British Columbia. There is global interest in how we approach and practice accountability for privacy. At the same time, sharper focus has been cast on the pivotal role that accountability plays in ensuring that privacy law balances the sometimes conflicting interests of individuals and businesses.

In 2013 the OECD published a revision to the guidelines on privacy protection that provide the foundational principles to privacy protection in Canada and in B.C. law.[5] The revised guidelines include new sections addressing accountability, including:

- new and extensive guidance on implementing accountability, including highlighting the importance of breach notification and demonstrable privacy management programs; and

[5] OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79], at Parts Three and Four.

- guidance on the free flow of personal information across borders and legitimate restrictions on those flows, which are part of an organization remaining accountable for the personal information in its custody and control regardless of where it is stored.

If there is one aspect of PIPA that requires modernizing it is in this area of accountability to keep pace with developments in other jurisdictions and the foundational principles upon which our law is based. Amendments to our legislation must remain current with developments in this area both internationally and at home. Such amendments would set up more clearly for organizations what they need to do to comply with PIPA and would provide people in B.C. with greater trust and confidence in the management of their personal information. The next section of this submission describes how mandatory breach notification amendments to PIPA would promote accountability and keep PIPA in step with legislative developments in Canada and in Alberta.

➢ MANDATORY BREACH NOTIFICATION

As I outlined in my May 28, 2014 submission to the Committee, placing a mandatory duty in PIPA to notify the Commissioner and the affected individuals in the event of a privacy breach can ensure protection of the privacy rights of individuals in B.C. Privacy breaches are breaches of the security safeguards that an organization puts in place to protect the personal information in its custody or control. They are also referred to as security breaches, and in the context where they result in the personal information of individuals being compromised they are also breaches of privacy.

Privacy breaches highlight the vulnerability of personal information when it is collected and stored, particularly when it is done in vast quantities. Breaches expose British Columbians to identity theft, financial harm and reputational harm. Recent large scale breaches involving organizations include Target, eBay, Home Depot and the Apple iCloud celebrity hacking scandal.

Although some organizations contact my Office when a privacy breach occurs, this does not always happen. In fact, organizations may not inform my Office or affected British Columbians when they have a privacy breach. There are some circumstances where the general obligation under section 34 may be interpreted to require notification where it would be a reasonable security measure to prevent, for example, unauthorized use of personal information.

However, an organization may believe that reporting a breach will be costly or harm its reputation, which can result in delays in notification or even a failure to notify altogether. This can have a cascading effect on potential outcomes to the breach: it means affected consumers are not able to take necessary steps to mitigate and prevent

harm, police will not have access to information that may be important to conducting an investigation into potential criminal activity, and my Office is not able to work with the organization to improve its overall privacy management program.

Individuals deserve to know when their personal information has been compromised. The decision to notify a consumer or an employee should not be based upon an organization's perception of the impact of a breach on its bottom line; instead it should be based on the impact of a breach on individuals. Mandatory breach reporting would also encourage organizations to implement stronger privacy and security measures that will protect their customer's personal information. In practice, section 34 of PIPA already requires organizations to protect personal information in its custody or control by making reasonable security arrangements. However, with over 380,000 organizations in British Columbia, my office simply lacks the resources to ensure all of these organizations are protecting personal information as required by PIPA. Mandatory breach notification will promote accountability and understanding that the more information organizations collect, the more information they will have to protect.

If an organization knows it must report a privacy breach to my Office and its customers, it will be much more inclined to invest the necessary time and resources to ensure that the personal information of British Columbians is protected. To not do so would place their brand and market share at great risk. Mandatory breach notification would motivate greater compliance with PIPA, build awareness of obligations and help to ensure organizations take proactive measures to protect customer data.

Providing for mandatory breach notification in PIPA would encourage organizations to harden their computer systems from ever-increasing cybersecurity threats, thereby reducing the likelihood of B.C. based companies experiencing costly breaches. Mandatory breach notification is also an important tool to enhance the fight against cybercrime, and its adoption would help British Columbia better position itself for success in the digital economy. In addition, alerting consumers that their personal information is vulnerable and exposed would reduce the chance they will become victims of identity theft.

The consensus opinion on adopting breach notification legislation in B.C. is indicated by the number of organizations that have made submissions in support of it: the BC Civil Liberties Association, the BC Freedom of Information and Privacy Association, the Canadian Bankers Association, the Canadian Bar Association, the Canadian Life and Health Insurance Association, the Canadian Medical Protection Association, Central 1 Credit Union and the Privacy Commissioner of Canada. I believe that the breach reporting requirements that follow would strike the necessary balance between the interests of businesses, consumers, and oversight by my office. Now is the time to adopt mandatory breach notification to secure the personal information of British Columbians.

➢ THE IMPORTANCE OF HARMONIZATION

Worldwide, mandatory breach notification has been acknowledged as one of the most effective tools to combat privacy breaches and protect the personal information of individuals. Last year the OECD identified that breach notification is an essential part of implementing accountability in privacy legislation.[6] The overwhelming majority of American states have passed mandatory breach notification laws, and the European Parliament is in the process of reforming its data protection laws to make breach notification mandatory. A number of our Pacific Rim trading partners have passed mandatory breach notification laws, including Mexico, Taiwan, and South Korea. The Australian government has placed it back on its legislative agenda with its Privacy Amendment (Privacy Alerts) Bill 2014.[7] In addition, China and Japan have sector-specific breach notification regimes.

Closer to home, the province of Alberta has had mandatory breach notification in place since 2010. In April this year Bill S-4, the *Digital Privacy Act* was introduced in the Senate. This Bill would add mandatory breach notification to PIPEDA, Canada's private sector privacy law. Adopting mandatory breach notification would facilitate harmonization with the above laws and allow us to remain substantially similar to PIPEDA if and when Bill S-4 is enacted.[8]

There are numerous reasons why harmonization with private sector privacy laws in Canada and abroad is critical. Given that businesses operate nationally or internationally, it is difficult and inefficient for businesses to have to comply with different requirements depending on whether they are federally regulated or provincially regulated. Harmonization facilitates both the understanding of organizations about their legal obligations and compliance with them. Moreover, in the absence of harmonization, large multinational companies may view doing business in B.C. as involving additional "hurdles" if our privacy laws are out of step with the rest of the world. The Canadian Bar Association, the Canadian Life and Health Insurance Association, and Central 1 Credit Union all recognized the importance of harmonization in this area in their submissions.

Harmonization also makes sense from a consumer's perspective. With large breaches being announced almost daily, there is a growing concern among citizens with the ability of businesses and organizations to protect their personal information. Customers

---

[6] OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79], at Part Three.

[7] Progress on this bill can be viewed at the Parliament of Australia's website for Bills of the current Parliament: http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query%3DId%3A%22legislation%2Fbillhome%2Fs958%22;rec=0.

[8] Bill S-4 has been through the Senate and was referred to the Standing Committee on Industry, Science and Technology before Second Reading on October 10th, 2014. The Committee starts its study of the bill on November 25th, 2014: http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=6748291&Language=E&Mode=1&Parl=41&Ses=2.

want to be able to shop for everyday products without having to worry about becoming the victim of identity theft. Mandatory breach notification will give consumers the comforting knowledge that if the businesses they patronize do suffer a security breach, they will be notified. This would allow them to take steps to protect their personal information and financial security. As it stands now, if a large company such as Target or Facebook were to suffer a massive security breach, they would be required to inform customers in Alberta, 47 American States, and countries across the Pacific Rim and Europe. However British Columbians, without mandatory breach notification, need not be informed.

➢ MODEL FOR MANDATORY BREACH NOTIFICATION

Should the Committee recommend mandatory breach notification for PIPA, there are several matters that must be considered. Detailed recommendations that mirror the language in Bill S-4 in order to achieve harmonization and substantial similarity are outlined below.

- **Definition of privacy breach:** A privacy breach should be defined to mean the accidental or unlawful loss of unauthorized access to or unauthorized disclosure of personal information, resulting from a breach of an organization's security arrangements referred to in section 34 of PIPA, or from a failure to make security arrangements.

  This language would complement that found in section 34 of PIPA. It reflects that the most common privacy breaches occur when security safeguards fail or when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed.

- **Threshold for notification**: An organization should be required to notify the Commissioner and affected individuals of any breach involving personal information under its control if it is reasonable in the circumstances to believe that the breach could create a real risk of significant harm to an individual. This is slightly different than the language in the Alberta PIPA (which only requires initial notification to the Commissioner) but it mirrors the language in Bill S-4.

  This threshold merits some discussion. On the one hand, the threshold must be low enough to capture breaches for which individuals and my Office will want to be notified. However, if all breaches were reported to consumers then my Office would quickly be overwhelmed and consumers could suffer "breach notification fatigue" whereby they would start to ignore notification. We also want a threshold that does not require organizations to notify where it would not be productive –

for example, a breach that was contained, or the loss of a disc with strong encryption. I believe the real risk of significant harm standard as we have seen it interpreted in Alberta strikes the right balance between these varied interests.

- **Timing of notification:** an organization should be required to, without unreasonable delay, provide notice to the Commissioner and individuals of any incident involving the loss of or unauthorized access to or disclosure of the personal information. It is important that affected consumers be notified as quickly as possible so they can take immediate steps to protect themselves from financial harm and identity theft.

- **Power of the Commissioner to order notification:** the Commissioner should have the power to order an organization to provide notification to individuals in circumstances where it is warranted but the organization has not already done so.

- **Form and contents of notification**: the organization should be required to report to the Commissioner and notify individuals in a prescribed manner and form. Notification to individuals must be conspicuous and given directly to the individual. An amendment to PIPA should provide a mechanism for notification to the individuals and the Commissioner to contain prescribed details [attached as Appendix A].

- **Duty of organizations to document breaches**: An organization should be required to keep and maintain a record of every privacy breach involving personal information under its control in accordance with any prescribed requirements. It should also be required to provide the Commissioner with access to, or a copy of, these records on request. In addition, organizations should be required to retain this information for at least two years so the records can be inspected if the need arises.

- **Power of the Commissioner to conduct investigations and audits**: The Commissioner should have the power to conduct investigations and audits of breach notification and security arrangement practices.

- **Penalties.** An organization that fails to notify affected individuals and the Commissioner of a breach once the organization determines that the breach has occurred should be guilty of committing an offence and be liable for a fine of not more than $100,000.

Introducing mandatory breach notification provisions into PIPA will improve the accountability of organizations in handling the personal information of British Columbians and will keep B.C from falling behind the development of privacy laws in a number of other jurisdictions.

Recommendation 1: Amend PIPA to include mandatory breach notification.

Recommendation 2: Amend PIPA to ensure that mandatory breach notification provisions in PIPA are in harmony with Alberta and federal models.

Recommendation 3: Amend PIPA to make mandatory breach notification comprehensive by addressing:

–– the definition of privacy breach;
–– the threshold for notification;
–– timing of notification;
–– a Commissioner power to order notification to individuals;
–– the form and contents of notification as prescribed through regulation;
–– a duty of organizations to document breaches;
–– a Commissioner power to conduct investigations and audits; and
–– penalties.

➢ PRIVACY MANAGEMENT PROGRAMS: MODERNIZING PIPA'S OBLIGATIONS IN ACCOUNTABILITY

The OECD Guidelines provide the foundation for private sector privacy protection in Canada.

As mentioned above, the guidelines were revised in 2013 and now set out a detailed framework for implementing accountability, including the role of privacy management programs. With the challenges that new technologies present to protecting the privacy of individuals in B.C., PIPA's existing general obligations on accountability should be updated to require organizations to be more specifically accountable for the personal information they process using privacy management programs.

PIPA currently requires organizations to develop and follow policies and practices that ensure they meet their accountability obligations under the legislation. However, it is apparent to my office that businesses would benefit from greater clarity about *how* they can address these accountability responsibilities. The answer is through the explicit obligation to develop a privacy management program.

It is difficult for a consumer to find out about privacy practices or to articulate a complaint about how their personal information is handled if the organization is not required to publish its privacy policies.

Yet this is at present the case under PIPA an organization is required to develop and follow policies and practices to meet its obligations under PIPA, but it is only required to make that information available on request.[9] A requirement for a published privacy policy would enable a consumer to identify an organization's policies and determine whether its operations are compliant with PIPA.

PIPA should be modernized in a way that explicitly requires organizations to have a privacy management program that:

- includes proper training for employees to ensure they are aware of their responsibilities under PIPA so they can better protect the personal information of consumers;
- is tailored to the structure, scale, volume, and sensitivity of the operations of the organization; and
- is monitored and regularly updated.

[9] PIPA Section 5.

Organizations should also be prepared to demonstrate, on request from my Office, the privacy management program they have in place to protect personal information.

These additions will complement the existing accountably requirements in PIPA: that organizations make reasonable security arrangements for personal information in its custody or control (section 34), that they designate one or more individuals to be responsible for ensuring organizational compliance with PIPA (section 4(3)), and that they develop a process for responding to complaints with respect to PIPA (section 5(b)). This will also ensure that B.C. is current with the global law and policy.

Recommendation 4: *How* organizations can implement accountability should be made more explicit under the Act. Amend PIPA to include a requirement that organizations adopt privacy management programs that:
–– make the privacy policies of the organization publicly available;
–– include employee training;
–– are tailored to the structure, scale, volume, and sensitivity of the operations of the organization;
–– is regularly monitored and updated; and
–– encompass existing obligations under the Act.

Recommendation 5: Amend PIPA to require that organizations be required to demonstrate a privacy management program to the Office of the Information and Privacy Commissioner upon request.

➢ Ensuring and Securing Third-Party Processing and Services

We have seen extensive growth in the use of cloud computing by organizations in B.C. and around the world. Rather than investing in local data storage infrastructure such as servers and data centres, organizations are more frequently turning to third-party vendors to store their customer and employee personal information. These third-party cloud-computing companies are often located in other countries. In this multi-jurisdictional environment 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.

We believe that PIPA's section 34 security arrangement obligations require organizations to be responsible for any personal information they send to third parties for processing or storage. To that end we have published guidelines on Cloud Computing for Private Organizations that describe these responsibilities.[10] However, these security obligations are not explicitly stated in PIPA and this may create confusion among businesses that believe third party providers are responsible for any personal information they receive. This could result in a company sending British Columbians' personal information to a discount cloud service lacking adequate security measures to protect personal information. Indeed, submissions to this Special Committee from the Alma Mater Society of the University of British Columbia and by Central 1 Credit Union have made the point that it would be helpful to organizations for this to be clarified in legislation.

PIPA should clearly state that when organizations transfer personal information to third-party processors or service providers, the organization must 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. Given the importance of this issue in the context of the increasing use of cloud computing this should be explicitly set out in PIPA as it is in PIPEDA.

Section 4.1.3 of the Schedule to PIPEDA should be used as a model. Individuals could rest assured that regardless of where an organization stores their personal information, it would be protected as required by PIPA.

Recommendation 6: Section 4 of PIPA should be amended, consistent with PIPEDA, to state 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.

[10] *Cloud Computing for Private Organizations (Small and Medium Sized Enterprises)*, 2012 at: https://www.oipc.bc.ca/guidance-documents/1437.

2.2 Bringing Accountability and Transparency to Disclosures Without Consent

➢ Disclosures Without Consent to Public Bodies and Law Enforcement

Section 18(1)(i) of PIPA authorizes an organization to disclose personal information for the purpose of complying with a subpoena, warrant or order made by a court. In addition, an organization may disclose personal information to a law enforcement agency without a warrant under section 18(1)(j). A number of organizations have made submissions about section 18 and the need for it to be interpreted in a manner that is consistent with *Spencer*, including the BC Civil Liberties Association, the BC Freedom of Information and Privacy Association, the Canadian Bar Association, and Open Media.

The range of disclosures permitted in section 18(1)(j) has been clarified in light of the *Spencer* decision. In *Spencer*, the Supreme Court of Canada made clear that a law enforcement agency requires a warrant to obtain information identifying an internet service subscriber in relation to otherwise anonymous internet use. This decision dealt with a section of PIPEDA that is similar to section 18 of PIPA.

As a direct result of *Spencer*, the largest telecommunications firms have recently changed their policies to be consistent with *Spencer*. They have both advised law enforcement officials they will no longer give basic customer information to police and security agencies without first seeing a warrant or equivalent authorization such as a court order.

British Columbians and Canadians are expressing concern about the extent of voluntary disclosures of personal information by private organizations to a government or law enforcement agency without a warrant, especially when individuals are not made aware of these disclosures. As I identified to the Special Committee in May, there has been and remains no way of knowing the number, scale, frequency of, or reasons for such disclosures. After *Spencer*, it is apparent there is a need to examine the authority for such warrantless disclosures.

At the same time, I agree with the BC Civil Liberties Association that such disclosures can happen in appropriate circumstances. For the purposes of section 18(1)(j), those appropriate circumstances should be when the organization itself is making a complaint to law enforcement about an offence under the laws of Canada or the province.

Private organizations would still be permitted under PIPA to disclose personal information:

- with a warrant, subpoena, or court order under section 18(1)(i);
- where required or authorized by law under section 18(1)(o); and
- in an emergency situation under section 18(1)(k).

Amending section 18(1)(j) to limit disclosures to organization-initiated complaints will bring PIPA in line with *Spencer*.

Finally, there should be greater transparency about the number of requests law enforcement makes to organizations and what the disclosures of personal information relate to. Organizations should be required to document and maintain disclosure logs and to report them in aggregate form whether or not they occur with a warrant. This public reporting could take the form of postings on the organization's website and the contents of such postings should be prescribed by regulation.

Transparency reports would be a mechanism for enhancing accountability and would allow the public, and our Office to see how much personal information organizations are currently disclosing. Three of Canada's telecoms have begun to publish transparency reports voluntarily. For the provincially-regulated private sector, these transparency reports should be mandatory.

➢ DISCLOSURES WITHOUT CONSENT FOR INVESTIGATIONS

Section 18(1)(c) of PIPA allows organizations to disclose personal information for the purposes of an investigation or proceeding without consent. While it does not require that these disclosures be made to other organizations, this is implied as its predominant application.

While the wording of section 18(1)(c) defines the situations where disclosure can take place, the circumstances within which it may be used is overly broad. We recommend that the wording in section 18(1)(c) be tightened to limit personal information disclosures without consent to cases where the disclosure is "necessary" for purposes related to an investigation or proceeding. If implemented, this section would be narrowed to permit disclosures without consent if "it is reasonable to expect that the disclosure with the consent of the individual would compromise an investigation or proceeding and the disclosure is necessary for purposes related to an investigation or a proceeding".

Spencer may have clarified the constitutionality of warrantless disclosures to police, but it did not do the same for disclosures between organizations. It is currently not possible for my Office or for the public to know how much personal information has been or is being disclosed without the knowledge or consent of individuals under section 18(1)(c). For this reason, transparency reports should also include information about disclosures to other organizations.

Recommendation 7: Amend section 18(1)(j) to limit disclosures to law enforcement to those that are initiated by the organization.

Recommendation 8: Amend PIPA to narrow the circumstances in which organization to organization disclosures can happen without the consent of individuals to circumstances where the disclosure is necessary (rather than "reasonable") for purposes related to an investigation or proceeding.

Recommendation 9: Amend PIPA to require organizations to publish transparency reports on disclosures made without consent.

2.3 Updating Order-Making Powers and Exceptions

➢ Order-Making Power on a Commissioner-Initiated Investigation

As I outlined in my May submission, PIPA does not currently permit the Commissioner to make an order in the absence of a complaint. The absence of this power is a gap in the enforcement powers of my Office and an inconsistency between PIPA and the *Freedom of Information and Protection of Privacy Act* ("FIPPA") where I have the power to make such an order. Individuals may be unaware of how their personal information is being collected, used, and disclosed and therefore unable to identify any possible contraventions of PIPA. My Office, with its expertise in privacy, is often better positioned to identify possible challenges to privacy and non-compliance with PIPA before the general public is even aware of the issues.

In a world where cookies on our personal computers report our surfing back to little-known entities and where large companies like Apple and Facebook collect and disclose our personal information to numerous third-party applications, individuals simply do not know where their personal information ends up. Many privacy policies

and user agreements often compound the problem by being lengthy and difficult to comprehend. Consumers often give up and just click "yes, I agree" without even reading or understanding these documents. This results in consumers being unaware about the repurposing of their data or if their data is even safe. Therefore they are often not likely to know there is a matter to complain about. Even where an individual has made a complaint, there may be a need to go beyond that one instance and launch a broader systemic investigation.

In today's marketplace, there is a power imbalance between the consumer and the commercial organizations. Too often, the burden of privacy protection is placed on the individual, which creates an uneven playing field in the implicit privacy negotiation between the consumer and company. By giving my Office the ability to initiate an investigation and make an order to protect consumers, we can help level that playing field. For these reasons, the Commissioner should have the ability to make an order as a result of a Commissioner-led investigation, even without a complaint. This would provide my Office with a necessary operational tool in the exercise of effective oversight.

Recommendation 10: Consistent with FIPPA, amend PIPA to give the Commissioner order-making power for Commissioner-led investigations.

➢ UNITED FOOD AND COMMERCIAL WORKERS DECISION

The Supreme Court of Canada's decision in *UFCW*[11] upheld the Alberta Court of Appeal's decision to quash a ruling of the Information and Privacy Commissioner of Alberta restricting the video taping of persons crossing a picket line. The Supreme Court found that PIPA violates the right of freedom of expression under the Charter, insofar as it restricts the collection, use, and disclosure of personal information for legitimate labour relations purposes.

PIPA is very similar to Alberta's law and therefore would likely suffer the same fate if put to a similar test before the courts. To address this issue, we recommend that the Legislative Assembly of British Columbia amend PIPA with a narrow exception that would permit the collection, use and disclosure of personal information without consent for the purpose of union picketing activity.

The Alberta Government and the Alberta Privacy Commissioner have recommended a similar narrow amendment in response to the Supreme Court decision. There have also

[11] [2013] 3 S.C.R. 733.

been submissions supporting such an amendment to this Special Committee to Review PIPA from the BC Civil Liberties Association, the BC Freedom of Information and Privacy Association, and the Canadian Bar Association. This type of targeted amendment would balance the protection of privacy with the freedom of expression in relation to union picketing activities.

On November 18, 2014, the government of Alberta tabled Bill 3: *Personal Information Protection Amendment Act*, 2014 for First Reading. The key amendment in this Bill is narrowly drafted and states:

> 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.[12]

While this amendment will of course be subject to legislative review and other democratic processes, I recommend that PIPA be amended based on what is enacted in Alberta. This will ensure continuing consistency between our two jurisdictions, consistent with the Canadian Bar Association's caution that it is best to avoid creating a "patchwork of privacy rules". While I am not aware of any particulars to be addressed arising from the BC context, I am confident that our own legislative process will be sufficient to discuss any issues that may need to be addressed.

Recommendation 11: Amend PIPA to add a narrow exception that would permit the collection, use and disclosure of personal information without consent for the purpose of Union picketing activity. The language of the amendment should be consistent with the language adopted by the province of Alberta's Bill 3: Personal Information Protection Amendment Act, 2014.

[12] The complete text of Bill 3 is available at: http://www.assembly.ab.ca/net/index.aspx?p=bills_status&selectbill=003&legl=28&session=3.

3.0 Stakeholder Recommendations

There are a handful of submissions to the Special Committee recommending amendments to PIPA to increase statutory authorizations for the collection, use, and/or disclosure of personal information without consent.[13] It is an internationally-recognized principle that individuals should have the ability to consent to the collection, use, and disclosure of their personal information. This principle lies at the core of PIPA (as it does PIPEDA and Alberta's PIPA). Recommendations that create further exceptions to this foundational principle will further diminish choice-based privacy protection for individuals in British Columbia. It is important for any requests of this nature to be closely scrutinized by legislators.

When the Committee considers additional authorizations in PIPA for collection, use, or disclosure without consent, I recommend that it consider the following:

- whether there is any other way to meet the need, either through another authorization in PIPA or through another means other than by diminishing the privacy of the individual involved;

- whether departure from the principle of individual consent to collection, use, and disclosure of personal information is clearly necessary, based on clear and persuasive evidence to address a pressing objective or concern;

- where such authorizations are deemed necessary, that any departure from consent is narrowly tailored such that it is:

    - limited to the personal information that is *necessary* for the purpose; and
    - limited to who may make such collections, uses, or disclosures.

In addition, I have comments about the following recommendations specifically made to the Special Committee.

3.1 Transfer of Personal Information to Public Bodies from Service Providing Organizations

A number of organizations raised concerns about the transfer of personal information from private sector organizations to government where those organizations provide services on behalf of public bodies.

[13] Central 1 Credit Union, Private Investigators Association of BC, BC Law Institute, Canadian Life and Health Insurance Association, Canadian Medical Protective Association, Ending Violence Association of BC, Insurance Bureau of Canada, and the Vancouver Island Strata Owners Association.

These concerns centered on government contracts that those organizations say require them to collect very sensitive client information that is in turn uploaded into a government electronic database.

The organizations state that this requirement undermines trust and creates barriers to provision of vital services. Organizations raising these concerns recognized the need to be accountable for the provision of these services and for government to properly monitor them. However, they are, in essence, of the view that they should not be obligated to turn over certain client information in order to be funded to provide those services.

I share the view of the organizations that it is critically important that citizens who need services have confidence their sensitive personal information be treated appropriately.

The challenge I face in providing the Committee with my views on this matter is a lack of detailed information before me about government policies that require disclosures by the organizations they contract with. I also do not have any examples of the contracts themselves to which the organizations have referred.

That said, whether PIPA or FIPPA applies to an organization's managing of personal information is determined by the facts of each case.

Where an organization is found to be "a person retained under contract to perform services for a public body"[14] then the organization is considered a service provider and FIPPA would apply. The definition for service provider is broadly defined to ensure that a public body cannot avoid its obligations under FIPPA by contracting out services to a private sector organization. PIPA explicitly states that where FIPPA applies PIPA does not.

I would observe that public bodies must make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.[15] What is reasonable may be context specific. For example, information about individuals accessing transition house services to escape abusive relationships must be secured in a different manner than someone accessing a service where safety implications are not at play. In practice this means the government information management systems such as the Integrated Case Management system must limit access to information to those for whom the information is necessary for the performance of their duties.

[14] Schedule 1.
[15] FIPPA section 30.

Where an organization is not considered a "service provider" but is disclosing personal information to government, it would be subject to PIPA. PIPA requires that there be consent from the individual from whom the organization has collected the information before disclosure can take place.

In light of the dual role played by some PIPA organizations – serving their own clients as well as providing services on behalf of the government – the interplay between PIPA and FIPPA may not be clear to some service providers and public bodies. My Office takes note of the need for guidance on the proper handling of personal information in these types of circumstances, and on how to comply with FIPPA or PIPA. We intend to provide such guidance in the near future.

The British Columbia Law Institute has raised a similar concern about disclosure by an organization to a public body, specifically with respect to assisted living facilities. It has asked for a "saving provision" in the *Community Care and Assisted Living Act* that deems that information collected under PIPA is validly collected under FIPPA where circumstances change for an individual who has shifted from independent living (subject to PIPA) to assisted living (subject to FIPPA) within the same facility.

While the British Columbia Law Institute seeks an amendment to an Act other than PIPA, such an amendment would effectively operate as a lawful authority to collect, use and disclose under PIPA. For the reasons already given above, I do not believe that such an amendment is necessary. An organization is required by PIPA to seek consent prior to disclosing personal information to government. Consent, so long as it is informed and consistent with the requirements of PIPA, could be collected at the time of entry into a facility or at the time of transfer within the facility. Information could also be newly collected under FIPPA once the individual has transferred to assisted living, in the manner set out above.

3.2 Central 1 Credit Union – Financial Abuse

Central 1 Credit Union submits that sections 18(1)(a) and (k) are not sufficiently clear to authorize credit unions to disclose personal information without consent in situations where financial abuse is suspected to be occurring and has asked for an exception to be added to PIPA for this purpose. I do not support its recommendation.

Section 18(1)(c) of PIPA already addresses this specific concern. In fact, the Canadian Bankers Association recommended to a committee reviewing the federal PIPEDA that it import the definition of "investigation" used in section 18(1)(c) of PIPA so that banks

could deal with suspected financial abuse without being in violation of privacy laws. That submission clearly implied that provincially regulated banking subsidiaries can already do this under PIPA's existing language.[16]

Central 1 Credit Union did not provide a compelling reason why PIPA should be amended, rather it simply said it should be amended for consistency with Bill S-4. However, as PIPA already permits dealing with suspected financial abuse such an amendment is unnecessary.

3.3 INSURANCE INDUSTRY

A number of insurance and risk management associations have made submissions to the Committee. Some of the recommendations were also submitted during the 2008 PIPA review, while others are new.

➢ INSURANCE BUREAU OF CANADA

Witness statements

The Insurance Bureau of Canada ("IBC") has asked that sections 12, 15 and 18 of PIPA be amended to provide that during the investigation and settling of an insurance claim, an organization should be allowed to collect, use and disclose a witness statement without the subject's knowledge and consent.

I support the Special Committee's 2008 recommendation that sections 12, 15 and 18 of PIPA be amended to allow the collection, use and disclosure without consent of personal information necessary for the insurer to assess, adjust, settle or litigate a claim under an insurance policy.

Access to witness Statements

The IBC has recommended that witness statements be exempt from access under section 23 of PIPA. It feels that the disclosure of witness statements may prejudice an insurer's ability to effectively investigate an insurance claim.

We continue to oppose any exception that would bar people from obtaining access to their own personal information. This recommendation runs counter to one of the main purposes of PIPA, namely the ability for a person to access their own personal information. Doing so allows an individual to determine what information an organization has collected about them, if an organization has inappropriately collected too much information about them, or if an organization has collected inaccurate information about them. We note that in their final report, the committee conducting the Special Review did not adopt this recommendation in 2008.

---

[16] *Submission by the Canadian Bankers Association to the British Columbia Special Committee to Review the Personal Information Protection Act*, February 12, 2008, at p. 1.

Discretion to disregard access requests
Section 37 of PIPA already allows the Commissioner to authorize an organization to disregard access requests that are repetitious or systematic in nature, as well as access requests that are frivolous or vexatious. The IBC has recommended that section 37 be expanded to include requests that "would amount to an abuse of the right to make those requests, or are not consistent with the purpose of the Act".

We believe that requests that would amount to an abuse of the right to make those requests, or are not consistent with the purpose of PIPA, would be considered frivolous or vexatious requests, and are thus already addressed in PIPA. That being said, we are not opposed to such an amendment as it would further align our legislation with Alberta's PIPA which contains similar wording.

➢ CANADIAN MEDICAL PROTECTIVE ASSOCIATION

Risk management advice
The Canadian Medical Protective Association ("CMPA") is seeking a specific amendment to section 18 of PIPA allowing disclosure of personal information without consent if the disclosure is required for the purpose of obtaining error or risk management services.

I don't support this amendment as it is unnecessary. In many cases we believe that doctors could provide the CMPA enough information to obtain risk management services without identifying the patient involved. In cases where personal information would have to be disclosed, the doctor could simply notify the patient involved and ask for their consent to disclose to the CMPA. In addition, the CMPA has not provided any evidence that this is a pressing problem and fails to provide any evidence to support this amendment in their current submission. We also note that the Special Review Committee did not support this amendment in 2008.

Use and Disclosure without consent: Expand the definition of a "proceeding" in section 18(1)(c) and broadening use in section 15(1)(c)
The CMPA has recommended that the definition of a proceeding in PIPA be amended to include an "anticipated proceeding" in relation to sections 15(1)(c) and 18(1)(c), which would permit the use and disclosure of personal information without consent for purposes related to an investigation or a proceeding. It has also recommended eliminating the requirement in these sections that such use and disclosure may occur if "it is reasonable to expect that the disclosure with the consent of the individual would compromise an investigation or proceeding". These amendments would expand the permitted disclosure of information without consent in the context of investigations and proceedings.

I have concerns about both of these proposed amendments. Sections 15(1)(c) and 18(1)(c) provide that the disclosure without consent is permitted if "it is reasonable to expect that the disclosure with the consent of the individual would compromise an investigation or proceeding". The CMPA proposes to eliminate this requirement altogether without demonstrating that it has been a barrier to effective proceedings or the defence of claims by the CMPA or its members. Further, this proposal would also eliminate this test in the context of investigations.

The ability of individuals to consent to the collection, use, and disclosure of their personal information is, again, a core tenet of PIPA. Over the past few years my Office has become increasingly aware that we do not know the extent to which organizations are making use of provisions authorizing non-consensual collection, use or disclosure. In light of this, my Office has proposed narrowing these provisions and providing greater transparency as to their use. While my Office did not object to expanding the definition of "proceedings" to include "reasonably contemplated" proceedings in 2008, I do not support further expanding this exception, including in light of the need for a better understanding of how often these provisions are being used.

➢ CANADIAN LIFE AND HEALTH INSURANCE ASSOCIATION

The Canadian Life and Health Insurance Association ("CLHIA") submission made recommendations regarding harmonizing mandatory breach notification with Alberta and ensuring that "fraud prevention" remain in section 18, and made additional recommendations:

Access rights and litigation

The CLHIA expressed the concern that plaintiff lawyers are making requests to insurance companies on behalf of their clients engaged in litigation proceedings with these same companies. They believe that these types of requests circumvent the discovery process and allow legal counsel to go on "fishing expeditions". They have recommended that PIPA be amended to refuse access where the disclosure of information would be likely to affect a judicial proceeding in which a person has an interest.

We have seen no evidence that access to personal information under PIPA is undermining the civil litigation process. As we have stated above, access to one's own personal information is a central tenet in PIPA and a person's right of access should not be extinguished simply because they are involved in civil litigation with an organization. We note that the committee conducting the Special Review in 2008 declined to put forward this amendment.

Access rights and medical information
CLHIA recommends that when an individual requests their medical information, an organization should be allowed to disclose sensitive medical information through a medical practitioner, rather than directly to the individual themselves. The CLHIA's concern is that that some sensitive information can only be fully understood and explained by a medical practitioner.

We see no need for this amendment. If the insurer is concerned about the reception of any sensitive medical information requested by an individual, they are authorized under section 5 of the regulations to disclose it to a medical practitioner for the purpose of obtaining an assessment as to whether the disclosure to the individual could "reasonably be expected to result in grave harm to the individual's safety or mental or physical health". The insurer can also request that same individual to consent to the disclosure through his or her medical practitioner.

3.4 PUBLICALLY AVAILABLE SOURCES OF INFORMATION

Central 1 Credit Union has proposed expanding the definition of a "prescribed source of public information" (section 6(1)(d)) to include social media and the Internet. Although this would provide some clarity to this section of PIPA, it could be problematic as many social media sites have various levels of privacy settings which provide users with the ability to select with granularity who can see what. As a result, what is "public" may not be clear.

For example, on Facebook, what the world can see and what your friends can see is often different if you have adjusted your privacy settings. This means a determination would need to be made as to what is considered publically available. Would it be what your friends can see? Or only what the world can see? The answer is not immediately clear.

I recommend that the Special Committee take care to consider the implications of such a change, including consideration of possible inadvertent impact on the individuals who are the most advanced users of privacy settings in social media.

3.5 SOLICITOR-CLIENT PRIVILEGE

Both the Law Society of British Columbia ("LSBC") and the Insurance Bureau of Canada ("IBC") have raised concerns about the protection of solicitor-client privilege afforded by section 23(a) of PIPA. These organizations brought up the same concerns in the 2008 review. In both instances, the Committee heard their concerns, but declined to adopt their recommendations.

➢ LAW SOCIETY OF BRITISH COLUMBIA RECOMMENDATIONS

The LSBC has again raised the question of whether the Commissioner's powers to examine documents in order to verify whether they are subject to solicitor-client privilege may be at odds with protection of the privilege.

PIPA gives the Commissioner responsibility for complaints and for review of the application of statutory exemptions to an individual's right of access to personal information. Those exemptions include section 23(3)(a), which allows an organization to refuse to disclose personal information in response to an individual's request for access to her or his own personal information if it is protected by solicitor-client privilege. To enable the Commissioner to perform the function of verifying the proper application of these exemptions, the Legislature conferred express powers and duties to conduct inquiries in private, to require the production of documents for examination and to review the information at issue in strict confidence. Section 38 therefore empowers the Commissioner to compel the production and examination of documents where an individual's access to personal information has been denied.

I do not agree with the LSBC's assertion that the Commissioner's jurisdiction to examine privileged documents may be inconsistent with section 3(3) of PIPA. Section 3(3) clearly states that nothing in PIPA affects solicitor-client privilege. In fact, we believe that section 3(3) has the effect of reinforcing the provision in section 38(3) that solicitor-client privilege is not affected by disclosure to the Commissioner. Therefore no inconsistency exists between section 3(3) and section 38 of PIPA.

The Commissioner is not an interested party and examines the documents only to determine the *validity* of the claimed privilege. This is the only way that the Commissioner can determine whether the claimed exemption is valid. The Commissioner does request the production of privileged documents in every instance, but only where it is necessary. The documents are not made public or put to any purpose other than verifying that this exemption has been properly applied.

In addition, if the Commissioner makes an order deciding against the privilege claim, the Commissioner does not disclose the documents. The order is directed to the organization claiming privilege, it is subject to an application for judicial review in the Supreme Court of British Columbia, and it would be stayed from the time the judicial review application is filed until the court orders otherwise.[17]

The Commissioner has had the power to examine and where necessary compel production of records protected by solicitor-client for 10 years in the private sector and over 20 years in the public sector. A considerable body of expertise has been built up in my Office during these decades and the process, which is efficient and timely, is working well. Through judicial review, the Supreme Court exercises a supervisory

[17] PIPA, s. 53.

function over my Office. The LSBC has offered no evidence to suggest that the present approach does not fully protect solicitor client privilege, which my Office recognizes is of fundamental importance.

I do not support this proposal to amend section 3(3) of PIPA and believe that an amendment is not necessary to fully protect the privilege.

➢ THE INSURANCE BUREAU OF CANADA

The IIBC recommends that section 23(3)(a) of PIPA be amended to specifically refer to "litigation privilege".

This change is not necessary because the reference to solicitor-client privilege in section 23(3)(a) already incorporates both legal professional privilege and litigation privilege. This has been confirmed in several orders from my Office under PIPA, including Orders P06-01[18], P06-02[19] and more recently in P10-02[20]. The phrase "solicitor-client privilege" has repeatedly been interpreted to include both kinds of privilege, legal professional privilege and litigation privilege.

In addition, numerous British Columbia court decisions[21] have affirmed that solicitor-client privilege encompasses both kinds of privilege. An amendment to section 23(3)(a) is therefore not necessary to specifically incorporate litigation privilege.

3.6 OTHER RECOMMENDATIONS TO THE SPECIAL COMMITTEE TO REVIEW PIPA IN 2008

There are a number of recommendations that were made to this Special Committee that were also made in the 2008 review by the same or other parties. I would like to affirm that my Office's position on these issues remains the same as in 2008. These include:

- Changing "minimal" to "reasonable" or introducing a schedule for fees for access requests (Central 1 Credit Union and one individual);
- Including a definition of "destruction" in PIPA (National Association for Information Destruction);

[18] An Incorporated Dentist's Practice, at: https://www.oipc.bc.ca/orders/1404.
[19] Victory Square Law Office & British Columbia Nurses' Union, at: https://www.oipc.bc.ca/orders/1405.
[20] Canadian Union of Public Employees, Local 1004, at: https://www.oipc.bc.ca/orders/1419.
[21] See, for example, *College of Physicians and Surgeons v. British Columbia (Information and Privacy Commissioner)*, [2002] B.C.J. No. 2779 (C.A.). Also see *Blank v. Canada (Minister of Justice)*, [2006] SCC 39, [2006] SCJ No. 39. The IBC refers to *Blank*, but does not note that the decision involved an interpretation of s. 23 of the federal *Access to Information Act*, specifically that the term "solicitor-client privilege" incorporates both types of privilege.

- The absence of labour relations or common law privilege (CUPE); and
- Records of professional client counsellors to have solicitor-client privilege extended to them (Kiwassa).

4.0 CONCLUSION

I would like to thank the Special Committee to Review PIPA for your work towards updating PIPA to keep pace with personal information management practices as they evolve with new technologies, and for the opportunity to contribute to this important work.

Organizations across B.C. can and do play an important role in taking a comprehensive approach to privacy in that many privacy issues can be dealt with through sound management of personal information. My Office works with organizations and individuals every day to promote and ensure sound personal information management practices by organizations. We look forward to seeing the recommendations from the Special Committee coming out of this review.

Summary of Recommendations

BREACH NOTIFICATION:

Recommendation 1:

Amend PIPA to include mandatory breach notification.

Recommendation 2:

Amend PIPA to ensure that mandatory breach notification provisions in PIPA are in harmony with Alberta and federal models.

Recommendation 3:

Amend PIPA to make mandatory breach notification comprehensive by addressing:

- **the definition of privacy breach;**
- **the threshold for notification;**
- **timing of notification;**
- **a Commissioner power to order notification to individuals;**
- **the form and contents of notification as prescribed through regulation;**
- **a duty of organizations to document breaches;**
- **a Commissioner power to conduct investigations and audits; and**
- **penalties.**

ACCOUNTABILITY

Recommendation 4:

***How* organizations can implement accountability should be made more explicit under the Act. Amend PIPA to include a requirement that organizations adopt privacy management programs that:**

–– make the privacy policies of the organization publically available;
–– include employee training;
–– are tailored to the structure, scale, volume, and sensitivity of the operations of the organization;
–– is regularly monitored and updated; and
–– encompass existing obligations under the Act;

Recommendation 5:

Amend PIPA to require that organizations be required to demonstrate a privacy management program to the Office of the Information and Privacy Commissioner upon request.

Recommendation 6:

Section 4 of PIPA should be amended, consistent with PIPEDA, to state 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.

DISCLOSURES WITHOUT CONSENT: TRANSPARENCY & ACCOUNTABILITY

Recommendation 7:

Amend section 18(1)(j) to limit disclosures to law enforcement to those that are initiated by the organization.

Recommendation 8:

Amend PIPA to narrow the circumstances in which organization to organization disclosures can happen without the consent of individuals to circumstances where the disclosure is necessary (rather than "reasonable") for purposes related to an investigation or proceeding.

Recommendation 9:

Amend PIPA to require organizations to publish transparency reports on disclosures made without consent.

ORDER-MAKING POWER ON COMMISSIONER-LED INVESTIGATIONS

Recommendation 10:

Consistent with FIPPA, amend PIPA to give the Commissioner order-making power for Commissioner-led investigations.

UNITED FOOD AND COMMERCIAL WORKERS DECISION

Recommendation 11:

Amend PIPA to add a narrow exception that would permit the collection, use and disclosure of personal information without consent for the purpose of Union picketing activity. The language of the amendment should be consistent with the language adopted by the province of Alberta's Bill 3: Personal Information Protection Amendment Act, 2014.

Appendix A

Prescribed details for notification of a privacy breach

1. Reporting to the Commissioner must be in writing and contain the following information:

   a) description of the circumstances of the breach;

   b) the date on which, or time period during which, the breach occurred;

   c) a description of the personal information involved in the breach;

   d) an assessment of the risk of harm to individuals as a result of the breach;

   e) an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the breach;

   f) a description of any steps the organization has taken to reduce the risk of harm to individuals;

   g) a description of any steps the organization has taken to notify individuals of the breach; and

   h) the name of and contact information for a person who can answer the Commissioner's questions about the breach on behalf of the organization.

2. Notice to individuals must be given directly to the individual and include:

   a) a description of the circumstances of the breach;

   b) the date on which or time period during which the breach occurred;

   c) a description of the personal information involved in the breach;

   d) an assessment of the risk of harm to individuals as a result of the breach;

   e) what steps individuals can take to mitigate these harms;

   f) a description of any steps the organizations has taken to reduce the risk of harm; and

   g) contact information for a person who can answer questions about the breach on behalf of the organization.