Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

STATUTORY REVIEW OF THE *PERSONAL INFORMATION PROTECTION ACT*

GENERAL BRIEFING FOR THE SPECIAL COMMITTEE TO REVIEW THE *PERSONAL INFORMATION PROTECTION ACT*

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

MAY 28, 2014

TABLE OF CONTENTS

1.0 INTRODUCTION

The *Personal Information Protection Act* ("PIPA"), enacted in 2004, mandates a comprehensive review of the Act by an all-party special committee of the Legislative Assembly at least once every six years.[1] This is the second occasion that a Special Committee of the Legislative Assembly has reviewed PIPA. The first Special Committee to review PIPA tabled its report and recommendations to the Legislative Assembly in April 2008. On February 25, 2014, the Legislative Assembly established a Special Committee to review PIPA for a second time.

This document provides the Committee with a brief history of private sector privacy law and a discussion of the current challenges to its effectiveness due to technological change and online security risks. It then gives a general overview of PIPA and the experience to date of the Office of the Information and Privacy Commissioner ("OIPC") in overseeing compliance with PIPA. The last section of the document is a brief discussion of key reform considerations that would improve the ability of the Commissioner to exercise effective oversight and enhance the transparency of disclosures of personal information.

1.1 THE IMPORTANCE OF PRIVACY

The term "privacy", not defined in British Columbia legislation, has different definitions. To some, it means anonymity, while still others believe it means the right to be unobserved. It includes the right to control access to your physical space, your body, your thoughts, your communications and your information.

A pernicious yet enduring myth is that privacy matters only to those who have something to hide. Most of us have nothing to "hide", yet still maintain the right to control the context, timing and extent of disclosures. Privacy matters because we all have the right to maintain a private life, separate and apart from our public life. We negotiate our identity in the world and choose to share pieces of ourselves with those we trust.

More than this, the essence of liberty in a democratic society is the right of individuals to choose, subject to demonstrably necessary and carefully tailored limits, what information they share with others.

Privacy matters because our physical and emotional well-being requires it. Imagine going to your doctor, dentist, priest or counsellor without any confidence that the information you supplied during those sessions would remain private. Privacy also matters because our economy depends on it. Imagine going to a credit union for a loan, to a lawyer to draw up a will, to a financial planner, to

[1] Section 59 of PIPA.

a property management company to rent an apartment, or to the internet to purchase a book online without any guarantees that the information you provided would be respected and kept confidential. As recent years have shown, the costs of fraud, identity theft and other misuse of our personal information are real, substantial and mounting. These losses harm individuals, but they can also harm economic activity and growth.

A large proportion of Canadians continue to worry about their privacy and have high expectations of strong privacy laws. They think that businesses and the government need to take their privacy responsibilities more seriously.

Many consumers are reluctant to shop online due to privacy and security concerns. Patients may withhold vital health information from their own physicians because of privacy concerns. The fall-out of concern about privacy is an erosion of consumer trust. In the face of privacy fears, consumers shop elsewhere or, certainly in the online context, provide false, inaccurate and incomplete information.

1.2 HISTORICAL CONTEXT

Private sector privacy law was necessitated by the need to promote global commerce and also protect consumer privacy. It gives assurance and confidence in data export to other jurisdictions. Its origins can be traced to European data protection laws passed in the early 1970s and guidelines in relation to transborder data flows developed by the Organization for Economic Co-operation and Development ("OECD") in 1980. In 1995, the European Union passed a Directive on data protection binding all member states that, among other things, prohibits the electronic export of personal data to any country that does not have an adequate level of legal privacy protections.

In response to the European Directive, the Parliament of Canada passed the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") in 2001. PIPEDA is deemed adequate to Europe's data protection rules.

The application of PIPEDA extends only to those provinces that have not enacted substantially similar legislation. When British Columbia enacted PIPA in 2004, it was declared substantially similar to PIPEDA. It therefore supplanted the Federal statute with the exception of banks, railways and telecommunication companies that are federally regulated. This substantially similar status is important for trade and for consumer confidence because it is part of a chain of assurance for international data flows.

Alberta enacted its own PIPA at the same time as BC. It is essentially the same as the BC legislation and was also declared substantially similar. Quebec has had private sector privacy legislation since 1994 and Manitoba passed a private sector privacy law in 2013 which is not yet in force.

South of our border things have developed somewhat differently. The United States takes a sector-specific approach to privacy, in contrast to the more comprehensive model adopted by Europe, Canada, and Commonwealth countries. In the U.S., privacy laws exist at the federal and state level and their number and variety is growing. Examples include the *Health Insurance Portability and Accountability Act* ("HIPAA") which creates national standards for electronic healthcare transactions and the *Children's Online Privacy Protection Act of 1998* ("COPPA") which regulates commercial websites and online services directed at children.

2.0 THE IMPACT OF TECHNOLOGY AND ONLINE RISKS

Because of sweeping technological change, there has been a seismic shift in the nature and amount of personal information held by private sector organizations since private sector privacy law was first enacted. We have also been radically transformed into a society where much of our lives are lived online. The result of this quantum leap in the collection, use and disclosure of information is new data security risks. In the face of this, strong privacy laws, active regulators and consumer awareness are more important than ever.

Six years ago, Twitter was a little known company, Facebook users numbered less than 100 million and smart phones had just been introduced. Today, Twitter has 500 million users; Facebook has a user base of 1.2 billion people and close to one-quarter of the worldwide population will use a smart phone monthly in 2014. Social media companies are only one kind of entity that know more about our habits, likes and location than could have been possibly imagined when MLAs last met to consider potential changes to PIPA six short years ago.

Examples of how technological change has altered the landscape include:

- Google Streetview and Google Glass – each present different challenges to privacy protection which privacy regulators have worked together internationally to address.

- Smart phones and mobile devices – enable us to carry large amounts of personal information around in our pockets. They can also allow third parties to collect massive amounts of data about us, whether it is where we are or how we are doing in Angry Birds.

- Cloud computing – individuals and organizations who use cloud computing to store personal information often have no idea where the data is physically being stored or who has access to it.

- Big data – many organizations are collecting and maintaining large amounts of personal information as they track the buying habits and preferences of their consumers. These large databases create tempting targets for cyber criminals and hackers. When the customer databases of companies like eBay, Target and Sony were breached the serious consequences were readily apparent.

The vast repositories of personal information collected in the private sector have not gone unnoticed by government. Reports recently came to light that in 2011 alone telecommunication companies disclosed almost 800,000 customer records to police and government agencies without a warrant. Although there are many legitimate situations where police and other law enforcement agencies need access to personal information, the scope, purpose and impact of these warrantless disclosures requires parliamentary and public debate.

It is generally acknowledged that it is private organizations, rather than governments, that hold the majority of personal information regarding individuals' activities online. In the face of this, we need to ensure PIPA keeps pace. Legal obligations to help ensure that that personal information is properly protected by organizations are a critical piece of consumer protection.

For any organization, privacy protection is essential to establishing and maintaining the trust and confidence of consumers. When personal information is handled respectfully, in an open and transparent manner, with strong, reasonable safeguards, and made accessible upon request, a continued positive relationship can be expected. Recently we have seen personal information become a tangible commercial asset with the rise of data brokers and data analytics. Businesses will want to build and protect their assets—and personal information, as an asset, is no different.

An example of the loss of trust and consumer confidence is the experience of the US retailer, Target, in a breach last year when hackers exposed the data of up to 110 million customers who had used credit and debit cards at the store. After the breach, Target's profit fell 46% in the fourth quarter of 2013. Target estimates the data breach cost them $61 million in the weeks after it was announced. Recently, Target announced the resignation of both its Chief Executive Officer and Chief Information Officer.

3.0 PIPA IMPLEMENTATION

3.1 DESCRIPTION OF PIPA

For the most part, PIPA fulfills its stated purpose of governing the collection, use and disclosure of personal information by private sector organizations in a manner that recognizes both the right of individuals to protect their personal information and the need for organizations to use that information for reasonable purposes.

Under PIPA, privacy means maximizing, wherever possible and to the extent that is reasonable, an individual's control over the collection, use and disclosure of his or her personal information.

PIPA contains rules about organizations' collection, use, disclosure and protection of individuals' personal information. In their interactions with law firms, credit unions, daycares and health care professionals, individuals choose to share different information with different organizations. PIPA preserves individual choice to control one's own personal information. It imposes legal obligations on organizations to collect personal information only with the consent of the individual or when the personal information has been provided voluntarily and the purpose of the collection is obvious. PIPA also gives individuals a right of access to, and correction of, their personal information held by organizations.

PIPA applies to "personal information", which it defines as information about an "identifiable individual". PIPA does not apply to the collection, use or disclosure of personal information for personal, home or family purposes, for artistic or literary purposes or for journalistic purposes (this protects freedom of expression for the news media).

PIPA is flexible, technology-neutral and principles-based. It contains a set of internationally recognized rules—called "fair information practices"—that govern the collection, use, disclosure and protection of personal information. For example, PIPA requires that:

- Organizations must obtain consent for collecting, using and disclosing an individual's personal information, except where PIPA excuses consent.

- Organizations must collect personal information only for reasonable purposes and must collect only as much as is reasonable for those purposes.

- Organizations must use and disclose personal information only for the purpose for which it was collected, unless the individual consents or PIPA permits the new use or disclosure without consent.

- Organizations must protect any personal information they hold with reasonable security measures.

- Individuals may request access to their personal information held by an organization.

- Individuals may request corrections to their personal information held by an organization.

3.2 MANDATE OF THE INFORMATION AND PRIVACY COMMISSIONER

The Information and Privacy Commissioner is an independent officer of the Legislature and has overseen PIPA since 2004. PIPA covers more than 380,000 for-profit and not-for-profit private sector organizations, including businesses, charities, religious organizations, associations, trade unions, political parties, strata councils and trusts.

PIPA gives individuals the right to ask the Commissioner to review matters where they are not satisfied with how an organization has

- responded to a request for personal information;
- responded to a request for correction of personal information;
- responded to a complaint about how it treats personal information; or
- followed or not followed any provision of PIPA.

A request for a review of an organization's response to an access request or correction of personal information must be made to the OIPC within 30 business days after the organization's decision. A dispute concerning the collection, use or disclosure of personal information, fees or a dispute on any other matter is termed a "complaint".

Our approach to complaints under PIPA is straight-forward. We investigate the circumstances of the dispute, consider the application of relevant sections of PIPA to those circumstances and, where practicable, involve the individual and the organization in efforts to arrive at a resolution. Individuals or organizations that are dissatisfied with these results have the option of asking the Commissioner to conduct an inquiry. At an inquiry, the Commissioner

or delegate issues a legally binding order that determines the outcome of the dispute. Orders are enforceable by a court of law, and can be appealed to the B.C. Supreme Court.

Complaints are on the rise. Compared to 2008/2009, complaints to my office have increased by 50% and requests for reviews and breach notifications have both increased by 60%. We have had an increase in requests for information related to PIPA by 50% over the previous year alone.

The OIPC receives privacy impact assessments from organizations for review and comment. These are an important education tool because we are able to guide organizations in their implementation of privacy and security frameworks and promote best practices. It allows us to influence the design of new systems before they are built and the implementation of new initiatives before they are launched.

3.3 GUIDANCE AND OUTREACH

An important role of the OIPC is to educate individuals and organizations about their rights and obligations under PIPA.

To that end, we have recently bolstered our online presence with a new website with improved access and functionality. The office has also entered the world of social media with over 600 followers on Twitter.

During the 2013/2014 fiscal year, we delivered 55 speeches to various private sector professional bodies and industry groups and met with many organizations to discuss their privacy concerns.

We co-host an annual PIPA conference with the Alberta OIPC. In the past seven years, these conferences have attracted approximately 2000 privacy practitioners and business leaders from the private and not-for-profit sector and provided invaluable training and awareness.

We partner with regulatory agencies from other countries and jurisdictions in our efforts to increase compliance with private sector privacy law. We live in a global world where large multi-national corporations exchange personal information with little regard to international borders. Recently my office, along with nine other international partners, outlined our privacy concerns to Google regarding their new product *Google Glass*.

We are a member of the Global Privacy Enforcement Network ("GPEN") which has examined website privacy policies and mobile applications in light of their compliance with national and provincial privacy laws. We are also an active member of the Asia Pacific Privacy Authorities ("APPA") and will be hosting a meeting of the Forum in Vancouver this December.

My office has produced a number of guidelines to assist organizations in implementing the requirements of PIPA. Some examples include:

- **Getting Accountability Right with a Privacy Management Program—** step-by-step guidelines for private sector organizations to build a privacy management program.

- **A Guide to B.C.'s PIPA for Businesses and Organizations—**helps organizations understand B.C.'s legal framework for access and privacy in the private sector; includes case examples, tips and a glossary of key terms.

- **Security Self-Assessment Tool—**helps organizations assess their security measures and offers guidance on minimum security requirements.

- **Cloud Computing for Private Organizations—**helps small and medium sized enterprises understand what their privacy responsibilities are and to offer some suggestions to address privacy considerations in the cloud.

- **Good Privacy Practices for Developing Mobile Apps—**outlines the privacy considerations when designing and developing mobile apps.

- **Practical Suggestions for your Organization's Website Privacy Policy—**outlines the basics of what an organization should consider when developing a website privacy policy.

- **Guidelines for Online Consent—**explains what is meaningful consent in an online context.

- **Guidelines for Overt Video Surveillance in the Private Sector—**sets out the principles for evaluating the use of video surveillance by organizations and for ensuring that its impact on privacy is minimized.

- **Guidelines for Social Media Background Checks—**provides rules for organizations that scan social media as part of their background check for employees, volunteers and election candidates.

- **Privacy Guidelines for Strata Corporations and Strata Agents—** assists strata corporations and strata agents in discharging their duties under the *Strata Property Act* in a manner that respects the privacy of owners.

- **Privacy Breaches: Tool and Resources—**includes key steps in responding to privacy breaches, privacy breach management policy templates, a privacy breach checklist, and a breach notification assessment tool.

3.4 PRIVACY BREACH INVESTIGATIONS

An important function of my office is to monitor and investigate breaches of personal information. A privacy breach generally means the loss of, unauthorized access or disclosure of personal information resulting from a breach of an organization's security safeguards. Under PIPA, an organization must put in place reasonable security arrangements to protect personal information in its custody or under its control. The most common privacy breaches happen when security safeguards fail or when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed.

Although not currently required by law, some organizations report significant privacy breaches to my office and seek guidance and advice. During the last fiscal year, a total of 50 privacy breaches were reported to my office by private sector organizations. When this occurs, we outline the organization's obligation under PIPA to contain the breach and also advise on notification of affected individuals.

Timely notification allows an organization to take advantage of the expertise available in my office and helps individuals mitigate the risk of identity theft and fraud. After the breach has been dealt with, we review security standards and help the organization put in place security measures to help prevent future breaches. Rather than being punitive, we seek to work with companies to mitigate any harm caused by the loss of personal information.

Examples of privacy breaches reported to the OIPC under PIPA include:

> **eBay—**Hackers raided its network three months ago, accessing some 145 million user records of which they copied "a large part". The records contained passwords as well as email addresses, birth dates, mailing addresses and other personal information, but not financial data such as credit card numbers. It is one of the biggest data breaches in history, based on the number of accounts compromised.

> **LifeLabs—**The Kamloops branch of LifeLabs sent a computer to their main office in Burnaby for servicing in January 2013, but when it was returned, the hard drive was missing. The hard drive held the results of ECGs, or electrocardiograms, gathered at three facilities between 2007 and 2013. The hard drive included personal information of 16,000 patients, including name, address, height, age, gender, the ECG results and health care number.

Another growing area of concern is unencrypted laptops and memory storage devices. There are high-profile examples of significant breaches in the public sector involving these devices, including:

> **University of Victoria—**A USB flash drive containing the payroll information of 12,000 employees was stolen from an office. The personal information stolen included the social insurance numbers and bank account information of the employees.
>
> **Ministry of Health—**There were three unauthorized disclosures of personal information on unencrypted portable storage devices. One of them contained 19 fields of health information, including the Personal Health Numbers of 4 million British Columbians.

Although these large breaches occurred in the public sector, they point to a growing trend of storing personal information on unencrypted portable storage devices and hard drives that are vulnerable to loss or theft. These portable storage devices can contain the personal information of thousands of British Columbians, yet they can be smaller than your thumb. When they are misplaced or stolen an individual can become the victim of identity theft in an instant. Even more concerning is the fact that many organizations are not using encrypted portable storage devices and hard drives to protect the personal information of British Columbians, even though this is a standard required by PIPA, the cost to do so is minimal and the benefit to the organization can be enormous. For example, had the University of Victoria used an encrypted USB flash drive prior to the theft, they could have saved themselves the huge costs they incurred in breach notification, credit bureau monitoring and related tasks.

3.5 PIPA Orders and Court Decisions

Under PIPA, the Commissioner has the ability to hold formal inquiries and issue orders that bind those involved. We believe the OIPC orders and court decisions in relation to PIPA have demonstrated a fair and balanced approach that protects individuals' rights without placing undue restrictions or onerous obligations on

organizations. Further, these orders and decisions have appropriately limited the application of PIPA to avoid unintended effects or intrusion into other areas.

Since 2008, the OIPC has issued orders providing important guidance on how PIPA should be interpreted and applied. Some highlights include:

- **Privacy of Employees—**In three separate orders, I found that an employer was authorized under PIPA to use GPS devices in company vehicles for purposes such as safety, vehicle maintenance and employee scheduling provided their employees were given notice of the use of the GPS devices. Subsequently, I found that an employer can monitor employees through the GPS functionality in cell phones issued to the employees provided they are given notice of the GPS monitoring. In the last decision, I ordered an employer to cease using GPS devices in company vehicles until proper notice of the use of GPS was provided to their employees. In all three cases I found that employers could not use GPS for ongoing employee surveillance.[2]

- **Privacy of Strata Owners—**We received a complaint that video surveillance in a strata condominium was in violation of PIPA. The Adjudicator found that video surveillance of exterior doors and the building parkade was permitted, but only for the purposes of preventing unauthorized entry, theft, threats to personal safety, or property damage. Video surveillance of the pool or the outside of a fitness room was not permitted, nor was providing a feed of the video to residents through their cable TV system. Further, PIPA required signs to be posted to notify individuals of the video surveillance.[3]

- **Privacy of Customers—**We received a complaint that a nightclub contravened PIPA by, as a condition of admission to the club, collecting and retaining their patrons' driver's license information by swiping licenses through an electronic card reader and taking a digital picture of the patron. We found that only limited information may be collected in this way for the purposes of improving safety and ensuring compliance with liquor laws.[4]

Two orders made under PIPA have been judicially reviewed by the Supreme Court of British Columbia. These court decisions have provided useful guidance

[2] Order P12-01, [2012] B.C.I.P.C.D. No. 25, Order P13-01, [2013] B.C.I.P.C.D. No. 23, and Order P13-02, [2013] B.C.I.P.C.D. No. 24.
[3] Order P09-02, [2009 B.C.I.P.C.D. No. 34.
[4] Order P09-01, [2009] B.C.I.P.C.D. No. 16.

as to when an individual not directly affected by an organization's actions has standing to make a complaint to the OIPC,[5] the procedure to be followed at an inquiry held under PIPA,[6] and the scope of the Commissioner's order making authority at inquiries under PIPA.[7]

4.0 MAJOR PIPA REFORM CONSIDERATIONS

4.1 MANDATORY BREACH NOTIFICATION

My main recommendation to the Committee in relation to the reform of PIPA is to add a mandatory duty to notify the Commissioner and affected individuals in the event of a privacy breach that creates a real risk of significant harm. This was recommended by the last Special Committee in 2008 and it was, in my view, its most important recommendation.

As it is now, some organizations contact my Office when a significant breach occurs even though they are not compelled to do so. We are able to give assistance and guidance as to the kinds of things an organization must do in the circumstances. However, I know that many organizations do not inform my office or affected British Columbians when there is a major privacy breach involving personal information. Organizations often believe that reporting a breach will be costly or harm its reputation. This concern can override the need to protect British Columbians from identity theft or reputational harm.

I note that in Alberta, which has mandatory breach reporting, the Office of the Information and Privacy Commissioner received 84 breach notifications in the 2012/2013 fiscal year. It is a concern that Alberta, which is smaller in size, but with express breach notification, is reporting almost 70% more private sector breaches compared to British Columbia.

British Columbians deserve to know when their personal information has been compromised. The decision to notify a consumer should not be based upon an organization's perception that its bottom line will be affected, but based upon the real risk of significant harm to the individual. Requiring organizations to notify affected individuals along with my office when a significant security breach occurs would allow British Columbians to take steps to reduce their vulnerability resulting from the disclosure.

---

[5] *Sochowski v. British Columbia (Information and Privacy Commissioner)*, 2008 BCSC 1390.
[6] *Economical Mutual Insurance Company v. British Columbia (Information and Privacy Commissioner)*, 2013 BCSC 903.
[7] *Sochowski* and *Economical Mutual Insurance Company*.

An organization that knows it must report a significant privacy breach to the regulator and its customers will be inclined to implement strong privacy and security measures. With over 380,000 organizations in British Columbia, we need incentives that encourage compliance with PIPA and ensure consumers are protected. Mandatory breach notification would drive compliance with PIPA, build awareness of obligations and help to ensure organizations take proactive measures to protect customer data. It would also allow individuals to take steps to protect themselves.

4.1.1 GROWING TREND

Mandatory breach notification is becoming a cornerstone of global privacy laws. In the United States, 47 of 50[8] states have passed mandatory breach notification laws. The European Parliament is in the process of reforming its data protection laws to make breach notification mandatory. Closer to home, the province of Alberta has had mandatory breach notification in place since 2010. Recently, the Government of Canada introduced the *Digital Privacy Act* (Bill S-4) which includes amendments that would add breach notification to PIPEDA. The proposed amendments to PIPEDA are similar to the language used in Alberta's PIPA.

Proposed amendments to Alberta's *Health Information Act* were recently introduced that include mandatory breach notification in relation to personal health information. These amendments were prompted by a high profile breach at Medicentre where a laptop computer containing unencrypted health information of 620,000 Albertans was stolen.

Unless British Columbia adopts similar amendments to PIPA, we risk falling behind other jurisdictions in consumer privacy protection. Moreover, if Bill S-4 becomes law we risk PIPA losing its substantially similar designation, leaving the BC law in legal limbo.

4.1.2 IMPORTANCE OF HARMONIZATION

There is a strong policy reason for harmonization among private sector privacy laws in Canada and abroad. 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

[8] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

provincially regulated. Harmonization facilitates both the understanding of organizations about their legal obligations and compliance with them. Moreover, in the absence of harmonization, BC could risk becoming a haven for bad actors.

Harmonization also makes sense from a consumer's perspective. It would be concerning to have a situation where affected consumers in Alberta were notified of a privacy breach—but consumers in BC affected by the same breach were not. This is a reality of the current regime.

4.1.3 MODEL FOR MANDATORY BREACH NOTIFICATION

Should the Committee recommend mandatory breach notification there are several matters that must be considered. These include:

- the definition of "breach";
- the threshold for notification;
- the timing of notification;
- how notification is provided;
- the contents of notification;
- exceptions to notification;
- duty to document breaches; and
- penalties.

It is also important to consider whether the Commissioner should have the power to order an organization to provide notification and conduct investigations and audits of breach notification practices.

Our more detailed submission in the Fall will include specific recommendations for a model of mandatory breach notification that balances consumer interests and is practical, flexible and scalable for the BC business environment.

4.2 ORDER MAKING POWER ON A COMMISSIONER-INITIATED INVESTIGATION

Unlike the *Freedom of Information and Protection of Privacy Act,* PIPA does not permit the Commissioner to make an order in the absence of a complaint.

Because data flows and data processing are seldom transparent, individuals are generally unaware of how their personal information is being collected, used, and

disclosed. Consumers are not informed about the complexities of data security or the repurposing of their data and therefore are not in position to even know there is a matter to complain about. Even if an individual were to make a complaint, there may be a need to go beyond that one instance and launch a broader systemic investigation. For these reasons, the Commissioner should have the ability to make an order as a result of a Commissioner-led investigation. It is an important tool in the exercise of effective oversight.

4.3 TRANSPARENCY REQUIREMENTS FOR WARRANTLESS DISCLOSURES [PIPA, S. 18(1)(J)]

PIPA authorizes an organization to disclose personal information for the purpose of complying with a subpoena, warrant or order made by a court [s. 18(1)(i)]. In addition, an organization may disclose personal information to a law enforcement agency to assist in an investigation or in the making of a decision to undertake an investigation, to determine whether the offence has taken place, or to prepare for the laying of a charge or the prosecution of the offence [s. 18(1)(j)].

The disclosure of personal information to a government or law enforcement agency without a warrant or in relation to a specific investigation is troubling. Individuals are not aware of these disclosures. There is no way of knowing the number, scale, frequency of, or reasons for, such disclosures. There is a lack of oversight and no established rules about what information can or should be provided without judicial warrant.

Given the risks to privacy, the broad authority in PIPA for warrantless disclosures should be reconsidered by the Committee reviewing PIPA.

At a minimum, organizations should be required to document and report warrantless disclosures. This public reporting could take the form of postings on the organization's website.[9] The contents of such postings should be prescribed by regulation.

Our submission in the Fall will provide specific recommendations for reform.

4.4 SUPREME COURT OF CANADA DECISION

In the November 2013 Supreme Court of Canada decision in *Alberta (Information and Privacy Commissioner) v. United Foods and Commercial Workers, Local 401,*[10] the Supreme Court upheld the Alberta Court of Appeal's decision to quash

[9] The Federal Privacy Commissioner has made this same recommendation for transparency about such extraordinary disclosures because of the overly broad authority to disclose for the purposes of law enforcement in PIPEDA.
[10] [2013] 3 S.C.R. 733.

a ruling of the Information and Privacy Commissioner of Alberta restricting the video taping of persons crossing a picket line. The Court found that to the extent that PIPA restricted the collection, use, and disclosure of personal information for legitimate labour relations purposes, it violates the right of freedom of expression under the Charter.

Both the Alberta Government and the Alberta Privacy Commissioner have recommended a narrow amendment that would permit the collection, use and disclosure of personal information without consent for union picketing activity. Our view is that the Legislative Assembly of British Columbia should amend PIPA in a similar fashion in order to balance privacy protections with freedom of expression related to union picketing activity. This would ensure consistency between our two jurisdictions, something that instruments such as the TILMA agreement have fostered.

5.0 CONCLUSION

The OIPC has provided guidance and expertise to both organizations and individuals about their obligations and rights under PIPA. However, much work remains to be done in terms of awareness and compliance. Given the massive expansion in the scale of personal information that organizations collect, use and disclose and online risks, it is imperative to have robust privacy laws and effective oversight. In BC, private sector privacy law needs to be strengthened to garner the attention of organizations and drive compliance. It also needs to meet the expectations of British Columbians that their personal information is properly protected.

Stringent legal obligations, particularly mandatory breach notification, would motivate organizations to implement strong privacy and data security practices. It would ensure that British Columbians will be made aware of security breaches involving their own personal information. Order making power in relation to Commissioner-led investigations would also strengthen oversight powers. A reconsideration of the authority to disclose personal information for law enforcement purposes, and reporting requirements for warrantless disclosures, would help to achieve the appropriate balance between privacy and public safety interests.

The single most significant tool to improve awareness and oversight, in my view, is mandatory breach notification. It would help to get privacy breaches out in the open. It does not have to be an onerous obligation on businesses. We need the right model for BC and it should be harmonious with other laws so that we are

on the same playing field as other jurisdictions. An express duty to notify would help to ensure that the personal information of British Columbians remains protected in a world that is experiencing unprecedented and rapid growth in technology where the security of data is increasingly at risk.

We recommend that the Committee hear from witnesses and receive submissions from an array of stakeholders, including representatives of organizations in the private sector to which PIPA applies. The Committee may wish to specifically solicit comments about the key reform considerations raised in this submission. We will respond to recommendations made to the Committee by others in our more comprehensive submission in the Fall.

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia