Review of the Personal Information Protection Act

Submission to the Standing Committee on Alberta's Economic Future

February 2016

Office of the Information and Privacy Commissioner of Alberta

On June 15, 2015, the Legislative Assembly of Alberta designated the Standing Committee on Alberta's Economic Future (Committee) as a special committee tasked with conducting a comprehensive review of the *Personal Information Protection Act* (PIPA) pursuant to section 63 of the Act. As part of its review, the Committee issued a *Discussion Guide*, opened a consultation process, and invited feedback from stakeholders.

I am pleased to make this submission to the Committee, which contains ideas, suggestions and recommendations for PIPA. This report's purpose is to ensure Alberta remains a leader in private sector privacy legislation across Canada and internationally.

Jill Clayton
Information and Privacy Commissioner of Alberta
February 2016

Contents

Introduction

The Office of the Information and Privacy Commissioner (OIPC) welcomes this opportunity to share its experiences regarding the administration of the *Personal Information Protection Act* (PIPA) with the Standing Committee on Alberta's Economic Future (Committee).

Albertans should be proud of this private sector privacy legislation. PIPA reflects its made-in-Alberta approach, as it came into force only after extensive consultation with Albertans and organizations to ensure that privacy compliance would not be onerous for small- and medium-sized businesses, yet would ensure the rights of Albertans to have their personal information protected. The Supreme Court of Canada has characterized PIPA as "quasi-constitutional", emphasizing the important role of this legislation in preserving our free and democratic society.[1]

Over the past decade, there has been a growing awareness among Albertans that they have the right to control their personal information. Albertans understand laws are in place which protect their personal information and give them rights of access. Organizations, generally, also have a better understanding of their duties to protect the personal information in their custody and control.[2]

Since PIPA's proclamation in 2004, there have been staggering changes in technology. The magnitude of personal information being collected by organizations around the globe, as well the ease with which it is used and disclosed, is unprecedented. It is an unfortunate fact that personal information data breaches now make headlines on a daily basis. While the repercussions of each data breach vary from mildly annoying to very serious, they all affect individuals. Everyone knows someone who has been affected by a breach, whether they are neighbours, colleagues, friends, family members or themselves.

PIPA Stats

From January 1, 2004 (when PIPA came into force) to December 31, 2015:

- 126 Orders/Decisions
- 26 Investigation Reports
- 3,138 files opened and 2,853 files closed
- 91% of files that could go to inquiry were resolved at the mediation stage
- 20% of the total OIPC caseload
- 60% of the total general inquiries (telephone calls)

Alberta has been a leader, both nationally and internationally, for its approach to private sector privacy. As a result of the last PIPA Review, Alberta became the first jurisdiction in Canada to require mandatory breach reporting in 2010. PIPA continues to serve as a model for other jurisdictions contemplating similar provisions.

A body of jurisprudence has also built around the interpretation of PIPA. Orders/Decisions and Investigation Reports provide guidance to individuals and organizations in understanding how PIPA works.

In addition, a generally consistent body of jurisprudence has been developed by other jurisdictions with substantially similar legislation. The Commissioner has worked closely with

1 *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 19.

2 These trends were explored in detail in the OIPC's *General Population Survey Final Report* and the *Stakeholder Survey Report* available at www.oipc.ab.ca.

the oversight offices for federal and British Columbia private sector privacy laws to harmonize approaches to privacy protection. For example, in 2011 the Privacy Commissioner of Canada and the Alberta and British Columbia Information and Privacy Commissioners signed the *Memorandum of Understanding with Respect to Co-operation and Collaboration in Private Sector Privacy Policy, Enforcement and Public Education*.[3] The three offices have also jointly published numerous resources, such as *Getting Accountability Right with a Privacy Management Program*.[4]

Not only is PIPA generally consistent with similar legislation across Canada, but historically, Alberta has seen benefit in attempting to harmonize, to the extent it is reasonable, the rules for privacy protection between Alberta's three primary statutes: PIPA, the *Health Information Act*[5] (HIA), and the *Freedom of Information and Protection of Privacy Act*[6] (FOIP Act). There is interplay among these three statutes: a significant number of employees in Alberta routinely deal with more than one of these laws in the course of their work. Using common terms, concepts and tests simplifies to a great extent the rules for collection, use and disclosure and ultimately improves statutory compliance by those many workers subject to these laws. Simplification and standardization also makes these laws more accessible to Albertans.

PIPA was designed to be technologically neutral – it requires organizations to consider the ways in which they collect, use and disclose personal information, regardless of the technological means chosen by those organizations. Despite the complexity of technological changes, PIPA has been and remains an effective law. It achieves an appropriate balance between protecting the privacy interests of Albertans and the legitimate collection, use and disclosure of their personal information by organizations for the purpose of providing goods and services. PIPA's continuing effectiveness is due, in part, to the wisdom of having a mandatory comprehensive review by a special committee of the Legislative Assembly every six years (section 63(1)(b)).

> *"The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy… legislation which aims to protect control over personal information should be characterized as 'quasi-constitutional' because of the fundamental role privacy plays in the preservation of a free and democratic society..."*
>
> - Supreme Court of Canada, *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 19.

The work of the Committee is very important. The Committee faces the challenge of making reasonable adjustments to PIPA to maintain its relevance without thwarting its objectives or making the legislation unduly complicated. The OIPC is pleased to provide this submission with recommendations to improve PIPA.

---

3 *Memorandum of Understanding with Respect to Co-operation and Collaboration in Private Sector Privacy Policy, Enforcement and Public Education,* https://www.priv.gc.ca/au-ans/prov/mou_e.asp.

4 *Getting Accountability Right with a Privacy Management Program,* https://www.oipc.ab.ca/media/383671/guide_getting_accountability_with_privacy_program_apr2012.pdf.

5 *Health Information Act,* RSA 2000, c. H-5.

6 *Freedom of Information and Protection of Privacy Act*, RSA 2000, C. F-25.

Non-Profit Organizations

In its 2007 Final Report, the all-party MLA Select Special PIPA Review Committee recommended that PIPA be amended to make the Act apply fully to all not-for-profit organizations, subject to a one-year limitation period.[7]

The OIPC supported the Committee's recommendation and continues to maintain its long-held position that all not-for-profit organizations should be fully subject to PIPA, as they are in British Columbia.

As noted in the previous PIPA review, the definition of non-profit organization in PIPA "has resulted in different treatment of similar organizations under PIPA (i.e. not-for-profit organizations that fall within the definition and those that do not). This, in turn, has resulted in differences in the way these organizations treat the personal information of their clients, employees, volunteers, and donors."[9]

Under PIPA, a non-profit organization is defined as an organization that is:

- incorporated under the *Societies Act* or the *Agricultural Societies Act*; or
- registered under Part 9 of the *Companies Act* (section 56).

These non-profit organizations have to comply with PIPA only when they collect, use or disclose personal information in connection with a commercial activity. This means that if the personal information of clients, donors, volunteers and employees was not collected, used or disclosed by the non-profit organization in connection with a commercial activity, the organization does not have to:

- advise individuals of the purposes for which it is collecting information;
- limit the amount of personal information it is collecting;
- make a reasonable effort to ensure the personal information it is using is accurate and complete for the particular purpose;
- make a reasonable effort to safeguard the information (e.g. store it in a secure place and ensure that the information is seen only by persons within the organization that have a need to know);
- destroy the information in a secure manner or render it non-identifying when it is no longer reasonably required for legal or business purposes;
- notify the OIPC of a privacy breach where there is real risk of significant harm to individuals; or
- grant individuals access to their own personal information held by the organization, to correct that information, or to tell them how it is using the information and to whom it has been disclosed.

Moreover, the organization's clients, donors, volunteers and employees do not have the right to complain to the Commissioner about the improper collection, use, disclosure or security of their personal information by the organization, or to ask the Commissioner to review the organization's response to their request for access to their personal information. The Commissioner

7 *Select Special Personal Information Protection Act Review Committee, Final Report* (November 2007) at p. 10.

8 Ibid.

also cannot require the organization to notify affected individuals of a privacy breach that presents a real risk of significant harm to the individuals.

There are 18,884 active societies under the *Societies Act*, 295 active agricultural societies under the *Agricultural Societies Act* and 2,125 active non-profit companies under Part 9 of the *Companies Act*.[9]

Not-for-profit organizations that do not fall within the section 56 definition of "non-profit organization" are fully subject to PIPA. These include religious societies, housing cooperatives, unincorporated associations, federally incorporated not-for-profit organizations, and organizations incorporated by private Acts. These not-for-profit organizations have the same obligations under PIPA as other organizations and businesses in Alberta to protect the personal information in their custody or under their control. Their clients, donors, volunteers and employees enjoy the same privacy protections and rights as the customers, clients and employees of businesses subject to the Act.

Additional inconsistencies arise for both the organization and individuals when a section 56 non-profit organization undertakes both commercial and non-commercial activities. For example, selling a membership or a fundraising list is a commercial activity. If a section 56 non-profit organization sells the personal information of its donors without their consent, the donors can submit a complaint to the Commissioner. However, the donors cannot complain if the organization publishes sensitive personal information about the donor without consent on its website.

Since PIPA was enacted, some 60 cases involving section 56 non-profit organizations have been brought to the OIPC; however, PIPA applied in only a handful of cases. In the remaining cases, the non-profit organization was not subject to PIPA because there was no commercial activity taking place. The Commissioner has not had jurisdiction in any of the self-reported privacy breaches sent to the OIPC by section 56 non-profit organizations. Yet, the privacy breaches suffered by these organizations are typical of those of other organizations, such as missing paperwork; computer system upgrades gone awry; and stolen unencrypted laptops containing sensitive personal information about many individuals, including banking and credit card information, criminal record checks, and social insurance numbers.

The increased emphasis by government on information sharing initiatives highlights the need to include all not-for-profit organizations under PIPA. Information sharing initiatives are frequently cross-sectoral, with a network of public, health, private and non-profit groups exchanging personal information for the delivery of services or programs. While public sector bodies, health custodians and private businesses are subject to privacy laws, the non-profit agencies will not be, if they fall within PIPA's definition of a non-profit organization and are not carrying out a commercial activity. However, many of these non-

9 Information retrieved from the Alberta Corporate Registry as of March 31, 2015 and from Alberta Agriculture and Forestry, http://www1.agric.gov.ab.ca/$Department/deptdocs.nsf/all/rsv14613

profit organizations are involved with vulnerable populations and handle very sensitive personal information about their clients. This is particularly true for those organizations providing social service or health programs, such as emergency shelters, drug or alcohol addiction counselling, and assistance programs for seniors and persons with disabilities. As the Commissioner has consistently stated, the benefits of information sharing should not come at the expense of privacy rights. All parties involved in information sharing initiatives should be regulated by privacy legislation and subject to the Commissioner's independent oversight.

The lack of statutory privacy protection may also impact service delivery as information sharing partners may be hesitant to share information with non-profit organizations that are not subject to privacy law.

There may be concerns that making PIPA apply to those non-profit organizations that are not currently subject to PIPA would add to their administrative burden. PIPA was originally developed with small- and medium-sized businesses in mind – to make informational privacy requirements easier to implement and comply with. If small- and medium-sized non-profit organizations were fully subject to PIPA, their obligations would be the same as for small- and medium-sized businesses. As was recommended in the previous PIPA review, implementation could be delayed one year to allow non-profit organizations to prepare for compliance. The OIPC is willing to work with Service Alberta to provide resources that would help non-profit organizations understand their obligations under the Act.

Recommendation

1. **That PIPA be amended to make the Act apply fully to all not-for-profit organizations, subject to a one-year transition period.**

Strengthening Accountability: Privacy Management Programs

Organizations subject to PIPA are responsible for personal information in their custody or under their control and are accountable for their compliance with PIPA. The "accountability principle" is one of the core privacy principles established by the Organisation for Economic Co-operation and Development (OECD) in 1980.[10] These privacy principles are the foundation for Canada's privacy laws, including PIPA and the federal *Personal Information Protection and Electronic Documents Act*[11] (PIPEDA).

PIPA was enacted with certain requirements to promote an organization's accountability. For example:

- organizations must designate one or more individuals to be responsible for ensuring the organization's compliance with the Act (section 5(3));
- organizations are required to develop and follow policies and practices that are reasonable to meet their obligations under the Act, and to make written information about those policies and procedures available upon request (section 6); and
- organizations must make reasonable security arrangements for personal information in their custody or under their control (section 34).

However, the privacy landscape has changed significantly since PIPA's enactment. Rapid advancements in technology allow individuals to share large amounts of personal information through social networks, e-mail, web logs, cell phone GPS signals, call detail records, Internet search indexing, digital photographs and wearable devices, and through online purchase transactions. Businesses (and governments) are able to collect, store and analyze vast amounts of data in ways never contemplated, to gather intelligence and identify trends to respond with better customer service, improved products and increased marketing. Privacy breaches have proliferated, with incidents often involving the personal information of thousands of individuals. And identity theft has become a real issue.

In this environment, individuals are much more aware of their right to control their own personal information and the importance of protecting it. They need and want to better understand how an organization is handling their personal information and what measures are in place to protect their privacy. This understanding is more critical when their information is being shared by partners in the private, public and health sectors for program or service delivery.

At the same time, organizations are more aware that personal information is one of the most valuable assets of an organization and that their business relies on maintaining the trust and confidence of their customers and employees by properly managing personal information. Organizations need a better understanding of how to build privacy and accountability into their operations – in short, how to implement a privacy management program that helps to minimize risks, strengthens privacy controls and supports compliance with their obligations under PIPA.

In their 2012 joint publication, *Getting Accountability Right with a Privacy Management*

10 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

11 *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5.

Program,[12] the Privacy Commissioners of Alberta, British Columbia and Canada provide guidance on what makes a strong privacy management program. The fundamentals include:

- appointing a person to be responsible for the development, implementation and maintenance of the privacy management program;
- developing and documenting internal policies that address the obligations under PIPA;
- educating and training employees in privacy protection;
- conducting privacy risk assessments;
- managing personal information handling by third party service providers;
- having systems in place to respond to individuals' requests for access to (and correction of) personal information or complaints about the protection of their information;
- having breach response and reporting protocols;
- informing individuals of their privacy rights and the organization's program controls; and
- monitoring, assessing and revising their privacy framework to ensure it remains relevant and effective.

The OECD has also recognized the importance of responsibility for compliance and revised its privacy guidelines in 2013 to include new provisions for implementing accountability within an organization. These provisions require the establishment of a privacy management program that:

- gives effect to the OECD Guidelines for all personal data under its control;
- is tailored to the structure, scale, volume and sensitivity of its operations;
- provides for appropriate safeguards based on privacy risk assessment;
- is integrated into its governance structure and establishes internal oversight mechanisms;
- includes plans for responding to inquiries and incidents; and
- is updated in light of ongoing monitoring and periodic assessment.

An organization must also be prepared to demonstrate its privacy management program to a data privacy enforcement authority, upon request.[13]

In its review of British Columbia's PIPA, the Legislative Assembly Special Committee agreed "that accountability is of critical importance to the effective implementation of PIPA" and recommended that organizations be required to adopt privacy management programs.[14]

The OIPC supports the implementation of privacy management programs by organizations. When

12 *Getting Accountability Right with a Privacy Management Program*, https://www.oipc.ab.ca/media/383671/guide_getting_accountability_with_privacy_program_apr2012.pdf.

13 *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

14 *Report of Special Committee to Review the Personal Information Protection Act*, February 2015, at p. 11. The programs are to be tailored to the structure, scale, volume, and sensitivity of the operations of the organization; make the privacy policies of the organizations publicly available; include employee training; and be regularly monitored and updated. In a separate recommendation, the Committee supported mandatory breach reporting by organizations.

submitting privacy impact assessments (PIAs) to the OIPC for review,[15] health custodians, public bodies and private sector organizations are asked to describe the management and policy structure they have in place to ensure ongoing privacy compliance. Modernizing PIPA by explicitly requiring that organizations have a privacy management program in place will strengthen organizations' ongoing compliance with PIPA and will ensure PIPA remains current and harmonized with developments in accountability in other jurisdictions.

The requirements of a privacy management program should be adaptable and scalable to the size of the organization and to the volume and sensitivity of the personal information that is in its custody or under its control. An organization should also be prepared to demonstrate its privacy management program to individuals and to the Commissioner, upon request.

Recommendation

2. **That PIPA be amended to require that organizations have a privacy management program in place and that organizations provide written information about their privacy management programs to the Commissioner and to individuals, upon request.**

15 PIAs are prepared when new organizational practices or information systems are proposed that may affect the personal information of individuals. They are due diligence exercises that identify privacy concerns so they can be addressed before implementation of the new practice or system. PIAs are mandatory under the *Health Information Act*, but public bodies under the *Freedom of Information and Protection of Privacy Act* and private sector organizations may prepare and submit PIAs as a best practice.

Disclosures Without a Warrant

PIPA currently limits disclosures to law enforcement bodies without consent to circumstances where there is an investigation being undertaken with a view to a law enforcement proceeding or where such a proceeding is likely to result (section 20(f)).

PIPA also permits disclosures without consent where the disclosure is authorized or required by a statute or regulation of Alberta or Canada (section 20(b)), or if the disclosure is reasonable for an investigation or legal proceeding (section 20(m)). Both "investigation" and "legal proceeding" are defined in PIPA and require a breach of an agreement, a contravention of a law, or a remedy available at law – or for a breach, contravention or remedy to be likely to occur (sections 1(1)(f) and (g)).

These existing disclosure without consent provisions (and related definitions) narrow the circumstances in which an organization can disclose personal information without consent to law enforcement without a court order, warrant or subpoena. As discretionary provisions, they permit, but do not require, organizations to disclose personal information to law enforcement bodies. And in all instances, the disclosure must be only for purposes that are reasonable, and limited to what is reasonable for meeting those purposes (section 19).

The *Discussion Guide*[16] raised the question whether PIPA ought to be amended in response to the Supreme Court of Canada's decision in *R v. Spencer*[17] (*Spencer*), or to address the issue of warrantless disclosures more generally.

In *Spencer*, the Supreme Court of Canada considered whether police could request subscriber information from an internet service provider (ISP) for the purposes of a law enforcement investigation without a warrant. In that case, the Crown argued that the federal PIPEDA authorized the collection of the subscriber information by the police because it authorized the ISP to disclose that information to the police. The Supreme Court of Canada clarified that even if PIPEDA authorized the ISP to disclose the subscriber information, the police needed their own authority to collect that information. In other words, legislation such as PIPEDA and PIPA might authorize an organization to disclose personal information to law enforcement in certain circumstances, but that authority to disclose is not authority for the law enforcement body to collect the personal information.

Rather, the law enforcement body requires its own authority to collect the information. This authority may come from various places: a warrant or court order, the federal *Criminal Code*, or public sector privacy legislation, such as the FOIP Act in Alberta. However, the authority to collect cannot be found in legislation that governs private sector organizations, such as PIPA.

If there is a desire to amend legislation to limit collection of personal information by law enforcement, the appropriate place to do so is in legislation that directly governs those law enforcement bodies, such as the FOIP Act in Alberta. Other legislation like the *Criminal Code* is federal legislation that can only be amended by that level of government.

16 Standing Committee on Alberta's Economic Future, *Discussion Guide: The Personal Information Protection Act*, January 2016.

17 *R v. Spencer*, 2014 SCC 43.

Further, while concerns about the amount and extent of information disclosed by organizations to law enforcement are reasonable, organizations also have valid reasons for such disclosures, for example, reporting a possible crime or aiding an investigation. Not all collections of personal information by law enforcement require a warrant or court order; whether such a warrant or order is required will depend upon the circumstances of the collection and type of information being sought. It is the responsibility of the law enforcement body to know whether it is authorized to collect personal information from an organization (or any other source).

When considering a warrantless request from law enforcement for personal information, organizations should, as part of their due diligence, ask the law enforcement body to identify its authority for making the request.

PIPA's existing provisions for disclosure without consent to law enforcement bodies are working well. They provide organizations with the flexibility to protect personal information in their custody or under their control, and to disclose to law enforcement where circumstances call for doing so.

Recommendation

3. **That no changes be made to PIPA's disclosure without consent provisions pertaining to disclosures without a warrant.**

Transparency Reports

At its very core, PIPA balances the right of an individual to have his or her personal information protected and an organization's need to collect, use and disclose personal information for reasonable purposes.

An individual exercises control over his or her own personal information by deciding which organization can have his or her personal information and for what purposes. When organizations are able to collect, use or disclose that personal information for other purposes without consent, the loss of individual control is mitigated by an organization's obligation to be open, transparent and accountable for the personal information in its custody or under its control.

> *"[W]hile it can be confidently stated that governments are seeking and obtaining far more access to personal data contained in company hands than has formerly been the case, the precise extent of that access is somewhat unclear. It is within this context that transparency reporting may have a useful role to play."*
>
> - International Working Group on Data Protection in Telecommunications[18]

There has been an increasing reliance by government agencies,[19] and particularly law enforcement, on personal information collected by private businesses about their customers and clients. Information may be disclosed by the private organizations without consent as a result of judicial warrants or legislative requirements, to assist with investigations or emergency situations, or on a voluntary basis. Familiar examples of disclosures of customer or client information to law enforcement or government agencies include disclosures by telecommunications companies; disclosures by banks, money services businesses and real estate brokers to deter money laundering;[20] disclosures of patron information by Alberta bars to peace officers upon request;[21] and disclosures by pawnbrokers.[22]

The significant privacy concerns and lack of transparency around such disclosures has led to several recent initiatives:

- Some Canadian, US and global private sector organizations have begun publishing

18 *Working Paper on Transparency Reporting: Promoting accountability when governments access personal data held by companies* (April 2015) https://datenschutz-berlin.de/attachments/1118/675.50.14.pdf?1435752521.

19 See Office of the Information and Privacy Commissioner of Alberta, *Deputizing the Private Sector: Requiring the Collection of Personal Information by Non-Government Entities for Law Enforcement or Other Purposes*, May 2015 https://www.oipc.ab.ca/media/387467/report_deputizing_private_sector_may2015.pdf.

20 *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17, http://laws-lois.justice.gc.ca/eng/acts/P-24.501/.

21 *Gaming and Liquor Act*, RSA 2000, c G-1; see also Office of the Information and Privacy Commissioner of Alberta and Alberta Gaming and Liquor Commission, *Guidelines for Licensed Premises: Collecting, Using and Disclosing Personal Information of Patrons* https://www.oipc.ab.ca/media/383672/guide_guidelines_for_licensed_premises_2009.pdf.

22 See *Business Watch International Inc. v. Alberta (Information and Privacy Commissioner)*, 2009 ABQB 10.

transparency reports voluntarily.[23]

- Since 2009, the Office of the Privacy Commissioner of Canada (OPC) has advocated for a reporting regime on personal information disclosures to government by commercial organizations. In 2015, the OPC issued a comparative analysis of transparency reporting by private sector companies.[24]
- In 2015, the Alberta OIPC commissioned an independent research paper, *Deputizing the Private Sector: Requiring the Collection of Personal Information by Non-Government Entities for Law Enforcement or Other Purposes*, to bring awareness to the subject.[25]
- In its 2014-15 review of British Columbia's PIPA, the Legislative Assembly Special Committee supported the position of the Information and Privacy Commissioner of British Columbia and recommended that organizations be required to document and publish transparency reports of disclosures made without consent.[26]
- In June 2015, Industry Canada (now Innovation, Science and Economic Development Canada) issued voluntary transparency reporting guidelines for private organizations.[27]
- In October 2015, the International Conference of Data Protection and Privacy Commissioner Offices issued a resolution calling on commercial organizations to maintain consistent records of government requests for access to customer and employee information and publish transparency reports outlining the number, nature and legal basis for those requests.[28]

PIPA requires organizations to be open and transparent about their policies and practices with respect to their management of the personal information of their customers, clients and employees (section 6). Organizations are also accountable for the personal information in their custody or under their control (section 5). While individuals have the right under PIPA to request information about how their personal information is and has been used by an organization and to whom it is being and has been disclosed (section 24(1.2)), there is no way for citizens in general, or the OIPC, to know the number, scale, frequency of, or reasons for disclosures without consent by private sector organizations to government or law enforcement agencies for non-business purposes. (By not knowing beforehand the frequency

23 Google www.google.com/transparencyreport; Apple http://www.apple.com/ca/privacy/transparency-reports/; Microsoft https://www.microsoft.com/about/business-corporate-responsibility/transparencyhub/; Rogers http://www.rogers.com/cms/pdf/en/2014-Rogers-Transparency-Report.pdf; Telus http://sustainability.telus.com/en/business_operations_and_ethics/governance_and_disclosure/transparency/; TekSavvy Solutions Inc. https://teksavvy.com/en/why-teksavvy/policies/legal-stuff/transparency-report; Sasktel http://www.sasktel.com/about-us/company-info/; MTS Allstream http://about.mts.ca/investors/governance/; Wind http://www.windmobile.ca/docs/default-source/default-document-library/2014-transparency-report-wind-mobileABF7DF074C25.pdf.

24 Office of the Privacy Commissioner of Canada, *Transparency Reporting by Private Sector Companies: Comparative Analysis* https://www.priv.gc.ca/information/research-recherche/2015/transp_201506_e.asp.

25 Ibid.

26 *Report of Special Committee to Review the Personal Information Protection Act*, February 2015.

27 See http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html.

28 See https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Transparency-Reporting.pdf.

with which their information is disclosed to government and law enforcement authorities, individuals are not able to make an informed decision as to whether to do business with that organization.)

Greater transparency and accountability in this area, as well as enhanced trust with customers and employees, would be achieved through periodic publication of transparency reports about disclosures to government and law enforcement agencies for non-business purposes. While some organizations may voluntarily publish transparency reports, prescribing the details of such reports ensures consistent and comparable data. The method of public reporting should be flexible to meet the nature of the organization's business; for example, reports could be posted on the organization's website.

Recommendation

4. **That PIPA be amended to address publication of transparency reports. Amendments should consider:**
   - **whether the reports should be limited to disclosures upon request of law enforcement or government agencies, or include disclosures made pursuant to legislation or on a voluntary basis;**
   - **the intervals for reporting; and**
   - **the minimum elements to be reported, such as the number and nature of the requests or disclosures, the legal authority for the request or disclosure, the response to requests (e.g. fulfilled, rejected, challenged), and the number of individuals or accounts involved.**

Freedom of Expression

In considering whether the current collection, use and disclosure provisions of PIPA that relate to trade unions are appropriate, it is important to keep in mind that PIPA does not limit expression except insofar as an organization uses individuals' personal information (without consent) – beyond this, PIPA has no effect on what trade unions may say.

In its decision in *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, the Supreme Court of Canada said that PIPA had a defect which needed to be legislatively remedied. The defect was the absence of a mechanism for balancing a union's constitutional right of free expression with the privacy interests protected by PIPA.[29]

The Alberta Legislature amended PIPA in a way that balances trade unions' rights of free expression and individuals' privacy interests.

As part of this review of PIPA, parties may propose that particular categories of organizations (e.g. trade unions, but possibly other categories of organizations which called for similar expressive rights) be exempted from PIPA entirely.

If an exemption from the Act for any particular category of organization were put in place, the result would completely change the approach of the Act from one of prohibiting unauthorized collection, use and disclosure of personal information to one of removing any constraints for a particular category of organizations, leaving them free to collect, use or disclose any individual's personal information at will, regardless of any consequences to their privacy or to themselves.

If this course were taken, an individual whose information was collected, for example by a trade union, would have no mechanism (except possibly an injunction or a civil suit – though there is currently no tort of invasion of privacy recognized in Alberta) by which to ensure his or her personal information was collected, used and disclosed only for reasonable trade union purposes, having regard to the nature of the information, its sensitivity, and the potential of harm to the individual from its use and dissemination.

Similarly, an individual would have no way to ensure his or her personal information was used and/or further disseminated in a reasonable manner having regard to these same considerations. For example, it might not be reasonable to post highly sensitive personal information where it might permanently remain on the internet to achieve some relatively minor trade union purpose, or where the information was of minor importance in achieving that purpose; however, the individual whose information it was would have no way to prevent this nor any recourse if it happened.

Permitting such a result would not ensure proportionality between the expressive goals of the organization and the protection of the individual's privacy, such as was contemplated by the Supreme Court of Canada when it spoke of balancing these factors.

29 *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 25.

Another important consideration is that, if exempted, other provisions of PIPA would not apply to those organizations.

For example, once an organization has collected personal information, section 34 of PIPA imposes an obligation on the organization to safeguard that information against risks of unauthorized access, collection, use, disclosure, modification or destruction. Organizations must destroy information in a secure manner or render it non-identifying when it is no longer reasonably required for legal or business purposes (section 35).

Organizations are also required by PIPA to report privacy breaches to the Commissioner and ultimately to notify affected individuals where there is a real risk of significant harm to individuals as a result of the loss, or unauthorized access or disclosure of personal information in the organization's control (sections 34.1 and 37.1).

Under PIPA, individuals also have the right to request access to their own personal information held by an organization, to request correction of that information, and to ask how the organization is using their personal information and to whom it has been disclosed. They may ask the Commissioner to review the organization's response to their request and can complain to the Commissioner about the improper collection, use or disclosure of their personal information.

Exempting any particular category of organizations from PIPA would remove these important privacy protections for personal information in the custody or under the control of the exempted organization and eliminate the rights given to individuals under the Act.

The OIPC offers no view as to whether there are any other categories of organizations whose expressive rights merit special protection under the Act; any such organizations may identify themselves, and explain the circumstances under which their expressive rights should override the personal privacy interests of individuals.

Recommendation

5. **At this time, the OIPC is not recommending any additional changes to PIPA concerning freedom of expression. However, should the committee identify any organizations as needing a special provision for their expressive rights then the OIPC recommends those organizations should be included within the scope of a provision that provides for the balancing of the purposes of the expression with the privacy interests of individuals.**

Notification of a Breach of Privacy

PIPA requires organizations to protect personal information in their custody or control by making reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction (section 34). A privacy breach occurs when an organization's security arrangements fail, and there is an incident involving the loss of or unauthorized access to, or disclosure of personal information (section 34.1(1)).

Unfortunately, breaches involving personal information have become increasingly common over the last decade. In fact, on most days, some high-profile breach or another is widely reported in the media; many more breaches do not make headlines.

On May 1, 2010, as a result of the last PIPA Review, Alberta became the first jurisdiction in Canada to require organizations to report breaches to the Commissioner where there exists a "real risk of significant harm" to an individual as a result of the loss or unauthorized access to or disclosure of personal information (section 34.1(1)).

An individual who becomes a victim of a breach may be subject to a wide variety of "significant harms", including: identity theft, financial loss, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, negative effects on a credit record, damage to or loss of property, and even bodily harm.

A "real risk" means the likelihood that the harm will result is more than mere speculation or conjecture; there must be a cause and effect relationship between the breach incident and the possible harm. It is an offence for an organization to fail to report a personal information breach to the Commissioner where there is a real risk of significant harm to affected individuals (section 59(1)(e.1)). The Commissioner has the power to require an organization to notify affected individuals of the breach (section 37.1(1)).

The primary purpose of data breach notification and reporting is to ensure that affected individuals are informed of incidents so that they can take steps to protect themselves against harm. Breach notification also provides an incentive for organizations to implement and update safeguards for the personal information in their control.

Since PIPA's mandatory breach notification provisions came into force, the Commissioner has made publicly available all decisions where a real risk of significant harm was identified and notification to individuals was required. Some of the recent privacy breaches and trends discussed in the OIPC's 2014-15 Annual Report are highlighted below:

- **Human error** – this includes inappropriate storage or disposal of personal information, and emails or faxes sent to the wrong person.
- **Insider misuse of personal information** – although many organizations have reasonable security arrangements in place to protect personal information against outside threats, they remain vulnerable to internal threats. The best defence against insider misuse includes access controls that limit users' ability to access personal information to their business need to know, coupled with an audit program to ensure employees are following the organization's rules.
- **Malware, hacking and e-commerce** – Malicious software and hacking continues to be a significant cause of privacy breaches Recent breaches reported to the Commissioner by online retailers involved

credit card payment information being exposed to unknown parties over lengthy periods.

- **Social engineering** – this refers to deceiving users or administrators of computer systems into revealing confidential information.
- **Failure to wipe hard drives** – despite previous Investigation Reports and guidance from the Commissioner's office, too many organizations still do not pay proper attention to securely deleting media before it is disposed of or re-sold.

Generally, the breach notification provisions in PIPA appear to be working well. In practice, the Commissioner has found that many organizations have already notified, or are in the process of notifying affected individuals when they report a breach to the office under PIPA.

The number of reported breaches has increased over the last few years, although it is unknown whether this is due to an increase in the number of incidents, or better awareness of the duty to report to the Commissioner, (or, most likely, both). To date, since the provisions came into force, approximately 550 breaches have been reported to the Commissioner.

The Commissioner does not have jurisdiction over all of the breaches reported to the OIPC, and not all of the breaches reported to the Commissioner pose a real risk of significant harm. Some organizations may choose to report to the Commissioner out of an abundance of caution, or in cases where they are not sure whether there is a real risk of significant harm. The Commissioner reviews all reported breaches to assess whether the Commissioner has jurisdiction, and if so, whether notification is required. Approximately 54% of the reported breaches where the Commissioner has jurisdiction, pose a real risk of significant harm to affected individuals.

Alberta's PIPA has set an example for the rest of Canada. In the recent legislative reviews of British Columbia's PIPA, and the federal PIPEDA, recommendations were made to add breach reporting provisions similar to Alberta's. In particular, both regimes have set the breach reporting threshold to be the same as Alberta's: a "real risk of significant harm". PIPEDA's breach reporting provisions, outlined in the *Digital Privacy Act* [30], will come into effect once regulations are finalized. Organizations subject to PIPEDA will be required to notify individuals and report to the Commissioner all breaches where it is reasonable to believe the breach creates a real risk of significant harm to the individual. The recommendations made by British Columbia's Special Committee to Review PIPA have not yet been drafted into legislation.

As stated above, the breach notification provisions are working well; however, there is a recurring issue concerning the relationship between an organization and its service providers. Under PIPA, it is the organization with control of the personal information that is required to report a breach to the Commissioner, and ultimately notify individuals, of privacy breaches where the breach creates a real risk of significant harm to individuals. However, it is often the case that a service provider to the organization has personal information in its custody (e.g. outsourced payroll services) but not under its control.

30 *Digital Privacy Act*, S.C. 2015, c. 32

Control rests with the principal organization to which it is providing the service. Absent a contractual provision with an organization, service providers have no obligation to report a privacy breach to the principal organization when an incident occurs. This can result in the principal organization not finding out about a breach, or in some cases finding out about a breach long after it has occurred. In such cases, there is a delay in notification or no notification at all to the Commissioner and the individuals who are facing a real risk of significant harm.

A requirement under PIPA for service providers (those organizations with personal information in their custody but not their control), to report a breach to the organization with control of the personal information would resolve this issue. A similar amendment to HIA was included in the *Statutes Amendment Act, 2014* [31] where affiliates are required to notify custodians of any loss of or unauthorized access to or disclosure of individually identifying health information (provisions not yet in force).

Recommendations

6. **That PIPA be amended to require organizations having personal information in their custody to notify the organization having control of the same personal information, without unreasonable delay, of any incident involving the loss of or unauthorized access to or disclosure of personal information.**

7. **That the *PIPA Regulation* be amended to require organizations to provide information to the Commissioner about the relationship with a service provider when a service provider is involved in a breach incident.**

31 *Statutes Amendment Act, 2014*, S.A. 2014, c. 8

Solicitor-Client Privilege

Solicitor-client privilege has become a critically important issue before the Commissioner's office.

Although the OIPC is not recommending any changes to PIPA at this time, background information is being provided so the Committee can better understand this issue and the Commissioner's concerns.

Background

Solicitor-client privilege applies to communications between a lawyer and a client, where legal advice is sought or given and is intended to be confidential. The purpose of solicitor-client privilege is to promote full and open communications between a lawyer and his or her own client. Generally, information that is protected by solicitor-client privilege is not admissible as evidence in proceedings and is not required to be disclosed.

PIPA and Solicitor-Client Privilege

Under PIPA, individuals have a general right of access to their own personal information, subject to exceptions and taking into account what is reasonable. For example, an organization may, but is not required to, refuse to provide access to personal information if "the information is protected by any legal privilege" (PIPA, section 24(2)(a)). This discretionary exception to disclosure under section 24(1)(a) includes information protected by solicitor-client privilege. If an organization applies an exception to disclosure, such as solicitor-client privilege, to the personal information being requested, the individual requesting access can ask the Commissioner to review whether the organization properly applied the exception.

The power of the Commissioner to review an organization's response to an access request is among the Commissioner's most important functions. PIPA is based on the concept that an individual has the right to control his or her own personal information, and the access rights enshrined in PIPA allow individuals to exercise this right of control. Access allows an individual to know what personal information an organization has about them. When an organization applies an exception, the Commissioner must have the ability to review the records being withheld from an individual.

Under PIPA, an individual is entitled to access only his or her personal information. In many cases, the information in a lawyer's file is not about an individual and is therefore not personal information and not subject to an access request. Commissioner's orders have confirmed this. There is no reason for an organization to rely on solicitor-client privilege to withhold information that an individual has no right to access to begin with.

In those cases where records are subject to an access request, experience has shown that organizations' claims of solicitor-client privilege are not always correct. In many cases, the Commissioner can make a determination as to whether the exception applies based on evidence from the organization about the record, but sometimes it is necessary for the Commissioner to review the record itself to determine whether an exception has been properly claimed.

The Commissioner's power to review records is set out in section 38(2) of PIPA under which "the Commissioner may require any record to be produced" and "may examine any information in a record". Section 38(3) of PIPA requires an

organization to produce a requested record to the Commissioner, "notwithstanding any other enactment or any privilege of the law of evidence". This phrase: "any privilege of the law of evidence" is used in many other access and privacy statutes in Canada.[32]

Until recently, courts across Canada had consistently held that "any privilege of the law of evidence" included solicitor-client privilege.[33] The Alberta Court of Appeal, however, in *University of Calgary v. JR*,[34] held that "any privilege of the law of evidence" did not include solicitor-client privilege. The Supreme Court of Canada granted the Commissioner leave to appeal the decision, and the case is currently scheduled to be heard on April 1, 2016.

As a result of the Court of Appeal's decision, there is a growing trend before the Commissioner's office where organizations withhold records at issue in an access request on the ground that they are solicitor-client privileged. The organizations then refuse to provide any further information about the records and refuse to let the Commissioner review the records to determine whether the exception has been properly applied. Accordingly, other than an organization's own assertion, there is no way to determine whether the exception has been properly applied. This has led to a growing number of cases where the Commissioner must issue a formal Notice to Produce the records at issue to an organization, and a growing number of cases ending up before the courts as organizations seek judicial review of the Notices to Produce.

Where it is necessary to review a record, the Commissioner will review it *only* to determine whether the privilege has been properly claimed; the Commissioner is not an interested party in the content of the records, other than to ensure that they are subject to the exception claimed. These records are not made public or put to any other purpose other than ensuring the privilege was properly claimed. Further, the Commissioner

---

32 **Alberta**: *Freedom of Information and Protection of Privacy Act*, RSA 2000, c. F-25, s. 56(3), and *Health Information Act*, RSA 2000 c H-5, s. 88(3).

Federal (Canada): *Access to Information Act*, RSC 1985, c. A-1, s. 36(2), and *Privacy Act*, RSC 1985, c. P-21, s. 34(2) Both Acts refer to "any privilege under the law of evidence".

British Columbia: *Freedom of Information and Protection of Privacy Act*, RSBC 1996 c. 165, s. 44(3), and *Personal Information Protection Act*, SBC 2003, c. 63, s. 38(5), which refers to "any privilege afforded by the law of evidence"

Manitoba: *Personal Health Information Protection Act*, CCSM c. P33.5, s. 29(5), and *The Freedom of Information and Protection of Privacy Act*, CCSM c F175 s. 50(3).

Ontario: *Freedom of Information and Protection of Privacy Act*. 52(1), and *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c. M.56, s. 41(4). Both Acts state: "despite Parts II and III of this Act or any other Act or privilege".

New Brunswick: *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05, s. 62, and *Right to Information and Protection of Privacy Act*, SNB 2009, c R-10.6, s. 62.

33 *District No. 49 (Central Coast) v. British Columbia (Information and Privacy Commissioner),* 2012 BCSC 427 at paras 49-50 and 55; *Newfoundland Labrador (Information and Privacy Commissioner) v. Newfoundland and Labrador (Attorney General),* 2011 NLCA 69 at paras. 37 and 52; *University of Calgary v. JR,* 2013 ABQB 652 at paras. 226 – 229 (overturned at CA, infra; leave to appeal to SCC granted).

34 *University of Calgary v. JR,* 2015 ABCA 118.

does not request the production of records over which privilege has been claimed in every case; in fact, the Commissioner has developed a detailed *Solicitor-Client Privilege Adjudication Protocol*, which sets out numerous steps regarding information to be provided regarding a claim of privilege before the organization will be required to produce the actual records. The Commissioner will require production of the actual records only as a last resort if all other steps have failed.

If the Commissioner finds that a record over which a claim of privilege has been asserted is not actually privileged, the Commissioner does not disclose it. The Commissioner must return all records to the organization after they have been reviewed (PIPA, section 38(5)). Where an exception does not apply to a record, the Commissioner will order the organization to disclose the record to the Applicant, and this order is subject to judicial review if the organization disputes the Commissioner's decision.

In the 2006-07 review of PIPA, the Special Select Committee "appreciated that, without the ability to examine the records, the Commissioner cannot provide a complete review of an organization's response to an access request."[35] Two changes were made to the legislation to create certainty for organizations concerning the protection of solicitor-client privilege when privileged records are provided to the Commissioner:

- Section 38.1 of PIPA was added to confirm that legal privilege would not be affected by disclosing the information to the Commissioner; and
- Section 41(3.2) was added to confirm that the Commissioner shall not disclose information subject to solicitor-client privilege to the Minister of Justice or Solicitor General.

At this time, the OIPC is not recommending any additional changes to PIPA. The OIPC is of the opinion that the current wording of the legislation "notwithstanding any privilege of the law of evidence" is sufficiently clear, and that it includes solicitor-client privilege. Further, this exact issue will be heard by the Supreme Court of Canada in April 2016. In the event that the Supreme Court of Canada provides guidance that affects the current interpretation of PIPA, the Commissioner will notify the Committee (or appropriate party) at that time.

35 Special Select *Personal Information Protection Act* Review Committee, Final Report, November 2007, page 35.

Commissioner's Standing Before the Courts

"Standing" refers to the right of the Commissioner to appear before a court when one of the Commissioner's decisions is being judicially reviewed.

PIPA requires the Commissioner to issue an order upon completing an inquiry. An order may, for example, direct an organization to provide, or not to provide, an individual with access to his or her own personal information, or to stop collecting, using or disclosing personal information in contravention of PIPA.

An order issued by the Commissioner is binding on the parties and is final (section 53). There is no right of appeal to the court; however, an individual or organization can apply to the Court of Queen's Bench for a judicial review of a Commissioner's order (section 54.1). Judicial review means that the Commissioner is subject to the law – a party may apply for a judicial review if they believe the Commissioner has made an unreasonable or incorrect decision, exceeded the Commissioner's jurisdiction, or has exercised the Commissioner's power in an arbitrary, unreasonable or discriminatory way.

A Court of Queen's Bench decision with respect to a judicial review is then subject to appeals to higher courts.

Currently, the Commissioner has no automatic right to appear before the Court of Queen's Bench or a higher court as a full or "true" party; rather, the Commissioner's standing must be determined by the court in each case. This uncertainty in every case before the courts is problematic because only the Commissioner has the ability to inform the court of the public interest and policy positions supporting the Commissioner's decisions. Further, the Commissioner is usually in the best position to help the court understand the complexities of the legislation at issue. Often these complexities may not be understood by the party challenging the Commissioner's decision, or may not be put forward to the court. In most cases the individual whose complaint or request for review is the subject of judicial review does not even appear before the court, so if the Commissioner does not appear, the court will hear only from the party disputing the decision at issue.

In some cases, it is necessary for the Commissioner to appeal a court's judicial review decision because the decision, while it may have focused on the limited issues between the parties, has a broader effect of undermining the public interest or a fundamental principle underlying PIPA.

Court Cases Regarding Standing

The Commissioner faces uncertainty in every court case as to whether the Commissioner will be allowed to participate, and if so, the extent of participation before the court.

The Alberta Court of Appeal recognized the Commissioner as being "very close to a true party" in *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)*[36] (*Leon's*). Importantly, in that case the Commissioner did not bring the appeal, but was responding to

36 *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)*, 2011 ABCA 95.

another party's appeal of a lower court decision. The Court of Appeal stated, "The Commissioner is very close to being a true party. It is unrealistic to think that the original complainant would have the resources or the motivation to resist the application for judicial review. If the Commissioner does not resist the judicial review application, no one will."[37]

However, more recently, that same court refused the Commissioner standing to appeal a decision. In *Imperial Oil v. Alberta (Information and Privacy Commissioner)*,[38] (*Imperial Oil*) the Alberta Court of Appeal refused to allow the Commissioner to initiate an appeal. The unfortunate result was that despite the very serious concerns the Commissioner had regarding the broader policy implications of the lower court's decision, the Commissioner had no standing to appeal those matters. Although the Imperial Oil case was decided under FOIP, not PIPA, it will likely act as a precedent in which the Commissioner is also prevented from appealing judicial review decisions under PIPA.

Currently, the Alberta Court of Appeal may grant the Commissioner standing as a party when another party brings an appeal (*Leon's*), but will not allow the Commissioner to bring an appeal (*Imperial Oil*). The situation is different again before the Supreme Court of Canada, where the Commissioner has been recognized as a full party in three cases, both where another party brought the appeal and where the Commissioner initiated the appeal.

A recent case from the Supreme Court of Canada reviewed the law on standing of administrative tribunals (see: *Ontario (Energy Board) v. Ontario Power Generation Inc.*, 2015 SCC 44). In this case, the Board had a limited statutory right of appeal in its enabling legislation (*Ontario Energy Board Act*, 1998, c15, Sch. B, section 33(3)). Another Ontario statute (*Judicial Review Procedure Act*, RSO 1990, c.J-1, section 9(2)), provides administrative tribunals, including the Information and Privacy Commissioner of Ontario, with standing before a court as a party on judicial review; however, the statute does not address the scope of participation; therefore, the scope remains in the Court's discretion.

A PIPA amendment addressing the Commissioner's standing before the courts should also address the scope of the Commissioner's participation. The Commissioner submits that PIPA include a provision that specifies the Commissioner has standing as a full party to appear and make submissions as a full party on judicial reviews of the Commissioner's decisions, and to initiate and appear on appeals from judicial review decisions on the same basis.

The proposed provision will bring consistency to the current uncertainty regarding the Commissioner's standing before the courts. It will ensure that the Commissioner's voice will be heard by the courts, and will allow the Commissioner to explain the public interest and the policies that the Commissioner is statutorily mandated to forward. It will also recognize the

37 Ibid at para 30.

38 *Imperial Oil v. Alberta (Information and Privacy Commissioner)*, 2014 ABCA 276.

Commissioner's important function as an Officer of the Legislature: the Commissioner does not just adjudicate disputes between parties; the Commissioner also makes policy, educates, initiates and investigates complaints (or can decline to investigate a complaint), and conducts a number of other functions. Unlike many tribunals, the Commissioner's adjudicative function is aimed towards building public policy, rather than resolving private disputes.

Recommendation

8. **That PIPA be amended to provide that the Commissioner has standing as a full party to appear and to make submissions as a full party on judicial reviews of the Commissioner's decisions, and to initiate and appear on appeals from judicial review decisions on the same basis.**

Costs

In Canada, regardless of the outcome of a judicial review, a tribunal rarely pays or is paid costs (see: *Brewer v. Fraser Milner Casgrain*, 2008 ABCA 160 at paragraph 23).

The Commissioner is not adverse to any other party in a judicial review proceeding. The Commissioner's primary role on judicial review is to assist the court in understanding the decision being reviewed, and in particular, the underlying policy and public interest on which the decision is based. As such, consistent with Canadian common law, the Commissioner should neither be awarded costs nor be subject to paying them. A provision in PIPA which formally recognizes the Commissioner as a party to judicial review proceedings, should not affect this general legal principle; however, enshrining this principle in a statutory amendment will resolve any uncertainty and will remain consistent with Alberta and Canadian law. Similar provisions are found in other tribunal statutes, such as the aforementioned *Ontario Energy Board Act* (section 33(5)).

The OIPC further recommends that in addition to the above statutory amendment granting the Commissioner standing before the courts, a further amendment should provide that the Commissioner is not subject to paying or receiving costs awards in respect of participation in a judicial review proceeding.

Recommendation

9. **That PIPA be amended to provide that the Commissioner is not subject to paying or receiving costs awards in respect of participation in a judicial review proceeding.**

Commissioner's Orders

After conducting an inquiry, the Commissioner is required to dispose of the issues by making an order (section 52(1)).

Section 52(2) lists the orders the Commissioner may make when the inquiry relates to the organization's decision on whether to give an individual *access* to his or her personal information or to provide information about the use or disclosure of his or her personal information. Section 52(2) was amended after the previous PIPA review to allow the Commissioner to make an order that the Commissioner considers appropriate when none of the listed orders would be applicable in the circumstances of a particular case(section 52(2)(b)).

Section 52(3) sets out the orders the Commissioner can make when the inquiry relates to a matter *other than an access request* referred to in section 52(2). However, there are instances where none of the enumerated orders in section 52(3) are applicable under the circumstances. For example, section 52(3)(a) allows the Commissioner to confirm that a duty owed under PIPA has been performed by the organization or to require the organization to perform the duty, but the inquiry might determine that there was no duty owed by the organization under the Act. In other situations, an issue might be moot so that there is no reason to make one of the specified orders.

A technical amendment to section 52(3) is therefore proposed – that section 52(3) be amended to include a provision similar to section 52(2)(b) to allow the Commissioner to make an order that the Commissioner considers appropriate when none of the orders currently listed in section 52(3) would be applicable.

Recommendation

10. That section 52(3) of PIPA be amended to allow the Commissioner to make an order that the Commissioner considers appropriate if, in the circumstances, an order currently listed in section 52(3) would not be applicable.

Summary of Recommendations

1. That PIPA be amended to make the Act apply fully to all not-for-profit organizations, subject to a one-year transition period.

2. That PIPA be amended to require that organizations have a privacy management program in place and that organizations provide information about their privacy management programs to the Commissioner and to individuals, upon request.

3. That no changes be made to the Act's disclosure without consent provisions pertaining to disclosures without a warrant.

4. That PIPA be amended to address publication of transparency reports. Amendments should consider:

    - whether the reports should be limited to disclosures upon request of law enforcement or government agencies, or include disclosures made pursuant to legislation or on a voluntary basis;
    - the intervals for reporting; and
    - the minimum elements to be reported, such as the number and nature of the requests or disclosures, the legal authority for the request or disclosure, the response to requests (e.g. fulfilled, rejected, challenged), and the number of individuals or accounts involved.

5. At this time, the OIPC is not recommending any additional changes to PIPA concerning freedom of expression. However, should the committee identify any organizations as needing a special provision for their expressive rights then the OIPC recommends those organizations should be included within the scope of a provision that provides for the balancing of the purposes of the expression with the privacy interests of individuals.

6. That PIPA be amended to require organizations having personal information in their custody to notify the organization having control of the same personal information, without unreasonable delay, of any incident involving the loss of or unauthorized access to or disclosure of personal information.

7. That the *PIPA Regulation* be amended to require organizations to provide information to the Commissioner about the relationship with a service provider when a service provider is involved in a breach incident.

8. That PIPA be amended to provide that the Commissioner has standing as a full party to appear and to make submissions as a full party on judicial reviews of the Commissioner's decisions, and to initiate and appear on appeals from judicial review decisions on the same basis.

9. That PIPA be amended to provide that the Commissioner is not subject to paying or receiving costs awards in respect of participation in a judicial review proceeding.

10. That section 52(3) of PIPA be amended to allow the Commissioner to make an order that the Commissioner considers appropriate if, in the circumstances, an order currently listed in section 52(3) would not be applicable.