Office of the Information and Privacy Commissioner of Alberta

CHECK AGAINST DELIVERY

Review of the Personal Information Protection Act

Jill Clayton, Information and Privacy Commissioner

Presentation to the Standing Committee on Alberta's Economic Future
October 15, 2015 | Edmonton, Alberta

Albertans Should Be Proud of PIPA

Good afternoon Chair, members of the committee. Thank you for the invitation to share the experiences of my office with respect to the Personal Information Protection Act or PIPA.

Let me begin by saying that Albertans should be proud of this piece of legislation. PIPA has been an effective law since proclamation in 2004. It achieves an appropriate balance between the privacy interests of Albertans and the legitimate collection, use and disclosure of their personal information by businesses for the purpose of providing goods and services. It was also purposefully designed to make privacy compliance as simple as possible for small- and medium-sized businesses.

Alberta is considered a leader in Canada and internationally for its approach to private sector privacy. We were the first jurisdiction in Canada to have mandatory breach reporting provisions, which were brought into effect in 2010, and we have served as a model for other jurisdictions contemplating similar amendments. Recent legislative reforms in other jurisdictions have borrowed from PIPA, including:

- British Columbia's review of their *Personal Information Protection Act*
- The federal *Digital Privacy Act* or Bill S-4 amended the *Personal Information Protection and Electronic Documents Act* to include a breach notification provision

- Manitoba's private sector privacy legislation has yet to be proclaimed but was heavily drawn from PIPA
- And Newfoundland and Labrador's *Access to Information and Protection of Privacy Act*

Another strength of this legislation is the mandatory review of the legislation by a special, all-party committee of the Assembly every six years. It's hard to believe that when this legislation was implemented, Facebook or Twitter didn't exist, we didn't have daily announcements of data breaches affecting millions of people, and there wasn't a federal law to limit the distribution of "spam".

When it comes to the collection, use and disclosure of personal information combined with the advancement of technology, it's appropriate and appreciated that we have the opportunity to review this legislation to maintain its relevance.

How PIPA Came to Be

To understand where PIPA came from, we have to go back to when the *Freedom of Information and Protection of Privacy Act* was proclaimed in 1995. At that time, it was one of the strongest laws of its kind in Canada. To complement the law, the provincial government developed an excellent suite of tools and resources and undertook extensive training of public sector workers.

In 2001, the *Health Information Act* was proclaimed. This followed more than two years of extensive consultation with health providers and health profession regulatory bodies.

By the time the Alberta Government decided to develop a private sector privacy law, we were able to build upon our extensive experience with public sector privacy when crafting PIPA.

These access and privacy laws have been characterized by the Supreme Court of Canada as "quasi-constitutional" as they define fundamental information rights of Canadians. As stated by the Supreme

Court: “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.”

What PIPA Is

Service Alberta will provide a more detailed explanation of the Act as the ministry responsible for the administration of PIPA, but I would like to illustrate a few concrete examples of what PIPA accomplishes:

- Have you ever noticed on a receipt that a majority of your credit or debit card number has been hidden? This was partly the result of an investigation in 2005 into an incident where files from businesses containing customers’ personal information were recovered during a police investigation. We ultimately got involved, and an organization was ordered to obtain the necessary technology to obscure credit card numbers printed on receipts, which set a precedent for other Alberta-based organizations.
- If you’ve ever been asked to check a box asking whether you would like to receive information about other products, that ability to opt-in to receive more information allows you to control how your information is used when sharing information with a business for a particular purpose.
- And if you’ve ever received a notice advising you that your personal information has been compromised, possibly offering you free credit monitoring services and providing advice as to the steps that you might want to take to protect yourself from identity theft or financial fraud.

These are all examples where PIPA has had an effect. Simply put, PIPA aims to protect the privacy of clients, customers, employees and volunteers by:

- Establishing the rules for the collection, use and disclosure of personal information by businesses and organizations in Alberta

- And requiring those businesses and organizations to have reasonable safeguards to protect that information, such as simply locking file cabinets or ensuring firewalls and other security measures are in place to keep hackers out of computer systems

As a measure to help individuals have control over their personal information, the Act generally operates on the basis of consent. There's also a general right of access to an individual's own personal information to know how it's being used or to whom it may have been disclosed. A right of correction of inaccurate or omitted personal information also exists.

That's the high level approach to private sector privacy legislation that PIPA achieves, but in order to ensure its effectiveness my office provides an oversight role as a regulatory authority of the Act.

The Role of the OIPC and Our Experience

I'm going to talk about the role of my office and our experience. As Commissioner, I have a number of powers and responsibilities under the legislation to ensure its purposes are achieved. I'll summarize each of these responsibilities with examples of my office's experience carrying out those responsibilities.

Requests for Review

When individuals request access to their information held by an organization and are not satisfied with the organization's response, they may request my office to review the organization's actions. For example, if someone did not receive all records that they thought the organization had in its possession or if the organization did not respond to the access request within the legislated timeline.

Under the legislation, organizations may charge a fee to process an access request. If someone is charged a fee and disputes the amount of the fee, my office can review the organization's fee estimate.

Privacy Complaints

Individuals can also make a complaint to my office if they believe their information was improperly collected, used or disclosed.

One of the more common concerns we receive from consumers is about the amount of personal information asked for by retailers when purchasing a product, or wanting to receive discount cards or memberships. A common complaint from employees has to do with the disclosure of their personal information regarding references for new jobs, workplace conflicts, or when medical information is being requested by or being shared within an organization.

In total, we have received more than 3,000 requests for review or complaints since PIPA was enacted in 2004. These involve all types of organizations from credit unions and energy companies to daycare providers and professional associations – any individual or organization involved in a commercial capacity is subject to the Act.

Mediations, Investigations and Inquiries

When my office receives a request for access or a complaint we will investigate and attempt to mediate the matter once an individual believes they have exhausted all options dealing directly with an organization. At the conclusion of an investigation or mediation, if the findings and recommendations are not accepted, the matter may be requested to go to inquiry, which is a formal process to resolve the matter that can result in a binding order. In total, there have been more than 120 orders under PIPA.

All orders are posted on our website. Just to provide a glimpse of what an order may include, in 2012, an adjudicator in my office found that Budget Rent-A-Car was contravening the Act when it was photocopying customers' driver's licences and was ordered to end the practice and destroy any such

information in its possession. This set a precedent for other rental car companies or similar service providers to follow.

Commissioner-Initiated Investigations

In addition to reviewing complaints, I can open investigations on my own motion. One example was following a fire at the Shaw Court building in Calgary in 2012. There were no complaints received; however, I was aware that personal information of Albertans was affected by the service outage the fire had caused. Alberta Treasury Branches, as a corporation, fell under PIPA and was subject to the investigation. Although no wrongdoing by the organization was found, the ability to come to this conclusion provided faith in the legislation. In such situations, there is oversight to ensure rules are being followed and it serves to educate other businesses that might be in similar situations.

Mandatory Breach Reporting

As mentioned earlier, another responsibility under the legislation is to review breaches that must be submitted to my office. I don't want to understate the importance of this provision as Alberta is a leader in Canada and internationally as a result of it.

Once a breach report is submitted to my office, I will then determine the significance of harm to an affected individual and determine whether the organization must notify those affected by the breach. Other than voluntary breaches reporting to affected individuals, only Albertans subject to a breach in the private sector have the legislated right to be notified in such a situation that a real risk of significant harm was identified, such as a harm of identity theft or financial fraud.

Recently, the federal private sector privacy legislation had a breach notification provision enacted; amendments to Alberta's *Health Information Act*, which have yet to be enacted, included breach reporting and notification; the committee tasked with reviewing British Columbia's PIPA has

recommended it; and Newfoundland and Labrador recently enacted breach reporting provisions making it the first to do so for public bodies in a Canadian jurisdiction. All have followed in PIPA's footsteps.

At times, human errors may cause a breach, such as leaving a door or cabinet unlocked, but other breaches can be malicious, such as stolen laptops or computer hacking. Either way, significant harms and direct losses to individuals often do result.

Headlines were made around the world recently with the Avid Life Media breach where users of the Ashley Madison website had emails among other details exposed by hackers. Like other breach notification decisions where a real risk of significant harm exists to Albertans, the breach report regarding Avid Life Media is published on our website. We did require the company to notify the affected individuals.

We rarely get through a day where another high-profile breach of personal information is not reported in the media and Albertans should be proud that we were among the first internationally to have legislated protection in the private sector in those situations where harm does exist to an individual. After all, since 2010, my office has received roughly one breach report every five days from an organization operating in Alberta. Over the past year, there have been more than 50 instances where I've determined that affected individuals must be notified by an organization that experienced a breach.

Education Mandate

An important aspect of my office's work is our ability to develop awareness of the legislation by informing and educating Albertans about their access and privacy rights. This starts with building awareness in organizations by providing guidance to organizations that are responsible for complying with the Act.

In the early days of PIPA, educating Alberta's organizations was a major focus of the office to ensure businesses understood their obligations under this new piece of legislation. Many of these organizations needed help with simply drafting a privacy policy let alone managing the complex issues that exist. During the first year, as was noted in the 2004-05 Annual Report, the office made 119 presentations to stakeholders and received nearly 4,000 questions about the Act.

In partnership with Service Alberta, we also developed many resources, including a guide for organizations that continues to be updated to maintain relevance. We have also collaborated with other privacy offices in Canada to develop resources, such as recent guidance documents on bring your own device programs and developing mobile apps. I maintain a Memorandum of Understanding with B.C's Information and Privacy Commissioner and the Privacy Commissioner of Canada that formalizes our cooperation in the areas of enforcement, policy, public education resources and information sharing.

In addition to educational resources, my office has also completed joint investigations with other offices, including one with the federal Privacy Commissioner in 2007 regarding a computer breach of TJX Companies – the parent company of Winners and HomeSense, among others – that affected the personal information of an estimated 45 million payment cards globally. One of the lessons learned from that investigation was for organizations to collect only what's needed and keep the information for only as long as required for the purpose. Lengthy retention periods and outdated security measures exposed personal financial information of those affected by that breach.

Comment on Legislative Reform

Another power I have under the legislation is what brings me here today, and that's my ability to provide comments and recommendations on legislative reviews and programs that have implications on access and privacy rights.

As I'm sure you can appreciate, the mandate of my office is varied, broad and constantly changing, which leads me to some of the current trends and issues we're seeing in private sector privacy.

Trends and Issues in Private Sector Privacy

As the legislation has matured, I recognize that organizations have become more aware of their responsibilities; however, the ability to collect and share massive amounts of information has become cheaper and easier, hackers have become more sophisticated when attempting to expose or exploit personal information, and a combination of those and many other factors has increased the complexity of the issues we deal with.

Some issues have remained since the beginning. As mentioned earlier, employee complaints and requests continue to be and have always been one of the most common issues we deal with. A subset of employee concerns is employee monitoring, particularly in drawing the line between what's personal and what's for employment purposes – and ensuring proper policies are in place to guide organizational and employee responsibilities. In 2013, my office issued an order pertaining to a situation in which an employee's personal phone calls were traced by his employer, yet the organization had no policy in place to restrict personal phone calls on devices supplied by the organization. Other employee monitoring issues centre on the use of workplace computers and emails.

Another issue that remains is video surveillance and maintaining the purpose for which the surveillance was implemented. My office has received many complaints where organizations have not thought through the implications of their surveillance. For instance, what happens when the camera in the front office captures a traffic accident on the street? What happens when an individual requests access to surveillance footage which contains not only their personal information, but that of numerous other individuals? What happens when a camera captures inappropriate behavior of employees outside of

the workplace? We continue to see many issues regarding proper notification and policies for surveillance activities.

Having said that, there are situations in which an organization has proven a legitimate purpose for a collection of personal information using video surveillance and ensured that information is reasonably safeguarded. In 2007, a decision allowed the Talisman Centre for Sport and Wellness in Calgary to continue its practice of using video surveillance in the men's locker room because it was found – and the organization proved – that the practice served a legitimate purpose to prevent theft in the locker room. To ensure the practice was legal, the organization properly secured the personal information collected and ensured it was used only to curtail the number of thefts.

Those highlight some of the issues that we have seen since the beginning and don't anticipate disappearing any time soon. However, there are other trends that have drawn more of our attention since the last PIPA review.

Information Sharing

One of the major issues we're frequently discussing is information sharing between the private sector, public sector and health sector. PIPA sets out many circumstances in which personal information may be shared by private sector organizations. There are, however, increasing pressures, particularly from government and law enforcement, for organizations to disclose even more information often without notice and consent.

At PIPA's core is the right for individuals to have control over and access to their personal information through various provisions, but if you're an individual and you don't know that an organization has collected your information and you don't know with whom it has been shared then it's impossible to

make a request to access that information and it's impossible to exercise your statutory right under PIPA to make a complaint about the collection, use or disclosure.

I've made a number of recommendations related to information sharing, most notably in the public sector, to ensure that individuals' access and privacy rights are upheld, but those recommendations are equally important in the private sector and include:

- Requiring that disclosures be documented
- Ensuring that individuals have an express, legislated right to ask for access to and a copy of disclosure notes
- And ensuring that they have the ability to come to my office and ask for a review if their questions are not being answered or if they're not satisfied with the response they receive

Non-Profits

Another issue that has not left my office's radar since the legislation was introduced has to do with the status of non-profit organizations under PIPA. As you may know, PIPA applies in a limited way to certain defined non-profit organizations and only to the extent that those organizations are involved in commercial activities. Since day one, my office has been advocating for the full inclusion of non-profit organizations under the legislation, as is the case in British Columbia.

Since PIPA was enacted, my office has had jurisdiction over one of the 24 requests for review that we received regarding non-profit organizations. What that means is that, essentially, an individual has requested access to their personal information from a non-profit organization to no avail. Seeing no other recourse, those individuals have sought a review from my office but we have found that the legislation provides no jurisdiction and, therefore, I have no authority to resolve those matters.

In terms of privacy complaints, 91% of non-profits subject to a privacy complaint were not covered under the legislation; in the remaining 9% of those complaints, it was found that the non-profit organizations were conducting a commercial activity meaning those organizations were subject to PIPA, and we could go in and attempt to work to resolve the issues.

It has also been found that I've had jurisdiction over 0% of the self-reported breaches received from a non-profit. While it's a good thing they're reporting matters to us, if we wanted to investigate or follow-up, we don't have jurisdiction to do so.

In 2007, the all-party committee tasked with review of PIPA recommended that non-profits be included but it was not included in amendments.

Considering these factors, I'm urging that the access and privacy rights of Albertans be extended to personal information collected, used and disclosed by non-profits under PIPA.

Solicitor-Client Privilege

Another issue that continues to be important in our office has to do with solicitor-client privilege. Although individuals generally have a right of access to their personal information, there are exceptions to that right of access. For example, organizations can refuse to provide access to information in a record that's protected by solicitor-client privilege. When my office reviews an organization's response to an access request, the review includes deciding whether an exception has been properly asserted.

Where an organization claims that a record is privileged, we have had some challenges obtaining access to those records in order to decide whether or not the privilege is being properly claimed. This is an issue that affects a significant number of cases in the office and is also currently before the courts, but I expect that we will have more to say about this issue in our formal submission to this review of PIPA.

A Path Forward for PIPA

Since the last review, the Alberta government made one amendment to the Act after a Supreme Court of Canada decision found the Act to be unconstitutional. An exception to consent was added for the collection, use and disclosure of personal information by a trade union in limited circumstances relating to a labour relations dispute. Between the time the Supreme Court deemed PIPA unconstitutional and when the Alberta government enacted amendments, I asserted that if PIPA was to lapse, Alberta would lose the unique benefits afforded by the legislation. With this review, I would like Alberta to continue to build a legacy for PIPA by balancing individuals' access and privacy rights with the legitimate needs of business to collect, use and disclose personal information.

As we all know, massive amounts of personal information are being collected, stored and shared at this very moment, so it would be easy to think that it's too difficult to deal with some of these issues, but I don't believe that's what Albertans want.

In our most recent general population survey, 97% of Albertans agreed that it's important to protect the privacy of personal information, yet only 27% felt their personal information was more secure than it had been five years prior. Meanwhile, organizations identified the pace of technology, mobile device security and hacking as among the most important issues they were expecting to deal with.

We all know someone or have personally been a victim of financial fraud. And most of us have heard of high profile breaches at Sony, Home Depot or Avid Life Media that are written in the headlines. Of course, these situations are troubling but at the very least individuals are recognizing that their information should be protected. Along the same lines, organizations are becoming more responsive to concerns from customers about the responsible collection, use and disclosure of personal information.

The issues in private sector privacy are as dynamic as they are complex. And as a society we're learning more each day about how vulnerable our personal information really is. These realities speak to a greater need for legislation that, at its core, is designed to ensure that individuals have control over their personal information and that they can access their information while balancing the legitimate needs of organizations and businesses. In my view, PIPA can be enhanced to maintain that balance, and Albertans should be and can be proud of the benefits that this legislation affords.

Thank you.