Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

SPEECH TO THE

SPECIAL COMMITTEE TO REVIEW THE *PERSONAL INFORMATION PROTECTION ACT*

NOVEMBER 26, 2014

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER FOR BC

Good morning Honourable Chair, members of the Committee.

With me today is Deputy Commissioner Michael McEvoy and oline Twiss Policy Analyst. Other members of my staff have joined us this morning and are seated behind me in the audience.

I want to begin by thanking you for the very important work the Committee is undertaking on behalf of all British Columbians.

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

However, in light of significant technological developments, carefully prescribed changes to PIPA are needed to give current expression to the core purposes of the legislation as it was enacted 10 years ago.

In my initial submission to the Committee, I described the vast changes that have swept over and influenced the way in which personal information has been collected and processed since PIPA was proclaimed.

Twitter was unknown, Facebook still resided in a college dorm room and “big” was never a word used to describe data. All of these developments and many others have resulted in dramatic changes in how organizations manage and use personal information.

Some of these changes are valuable to us socially and economically. They bring efficiencies to organizations and conveniences to individuals. They allow us to connect in an instant for personal or business matters. We have also seen advances in storing personal information, from local storage to the cloud, and in applying data analytics to information for all kinds of purposes.

It is cliché but true nonetheless that personal information is the new currency of our economy.

This is the world we now live in … one in which we must ask whether this legislation, now a decade old, requires updating to address these developments.

In 2004 when PIPA was enacted it was one of the leading pieces of privacy legislation in the world. The privacy principles enshrined in PIPA, based on those established by the Organization for Economic Co-Operation and Development, are fundamentally sound and as relevant today as they were then.

These foundational principles MUST remain at the heart of any changes to PIPA the Committee might recommend to the B.C. Legislature.

However, legislation is very much like a living organism. It must grow and change if it is to adapt to its environment.

In my four years as Commissioner, I have undertaken numerous investigations and received hundreds of complaints and requests for reviews under PIPA. I have assessed trends in the rest of Canada and around the globe where privacy authorities exist.

If I were to sum up in a single word what the current environment demands… and what all organizations must embrace… that word is ***accountability***.

Accountability means that companies are ethically responsible for the use and protection of personal information entrusted to them by citizens, clients and customers.

Accountability is analogous to the money we trust to banks and credit unions.

When you deposit your paycheque, the bank has to keep that money “safe” and only use or invest it based on your decisions.

Controls have long been in place in the financial sector to ensure these rules are followed, and there are various accountability and transparency mechanisms for

shareholders, board members, clients and financial regulators. And there is a report to the client on a regular basis.

Every month, you get a statement detailing your recent transactions. Every quarter, you get a statement describing how your investments grow or shrink.

Just as these controls exist in the financial sector, there is a demonstrated need for specific accountability measures in our privacy laws…

…including proper controls and management processes to protect personal data, clear rules for third-party data processing… and specific transparency and public reporting requirements when personal data is compromised, or disclosed to law enforcement.

My written submission provides a detailed description of the 11 recommendations I am making to the Committee.

If implemented, these changes would clarify an organization's responsibility to protect personal information (in other words, help businesses to comply with the law) and improve openness and transparency to the benefit of citizens.

A focus on accountability is very much a global movement. Lawmakers around the world are debating and adopting reforms to include specific legal requirements for businesses to create, and maintain, comprehensive privacy programs that span the entire organization.

Writing specific accountability mechanisms into PIPA would put BC on the leading edge of this global movement and put us on solid footing vis-à-vis other Canadian jurisdictions whose privacy laws are evolving to address the challenges of the digital age.

ACCOUNTABILITY – PRIVACY MANAGEMENT PROGRAMS

I'd like to begin by describing how PIPA can be amended to explicitly set out the tools and controls organizations must have in place in order to be held accountable for their personal information practices.

The **fundamentals** of accountability are prescribed in the current legislation.

Sections 4 and 5 of PIPA state that organizations are responsible for personal information under their control. It also states that they must have policies and practices in place to meet their obligations under PIPA and that they must designate an individual who is responsible for organizational compliance under PIPA.

When first enacted these were leading provisions on accountability in privacy in Canada.

However, it has become clear to my Office through our enforcement actions and discussions with organizations that many of them do not know how to operationalize the current accountability elements.

This has resulted in an observed lack of meaningful commitment to privacy protection. It is not unusual for us to see privacy policies gathering dust on a shelf rather than integrated into an organization's management of personal information.

Over the past several years, Canadian Privacy Commissioners have worked together to fill this knowledge gap and get businesses to commit to a CULTURE of privacy by providing detailed, scalable and practical guidance that gives businesses a roadmap to accountability.

The guidance is called "Getting accountability right with a privacy management program" and it provides building blocks to a comprehensive privacy management program.

The building blocks start with the fundamentals – creating a Chief Privacy Officer role. This person should sit at the executive table and should be empowered to lead the privacy agenda for the business in a similar manner as does the Chief Financial Officer.

Once this foundation is laid, program controls are necessary –training and education, risk assessment, policies and practices to ensure privacy is embedded in the DNA of the organization.

Finally there is ongoing assessment and revision—this is critical in light of changing threats and risks. The key is that privacy and data protection is not a one-time investment, or a one-off activity. It is an ongoing, evergreen process that must be done in a holistic way.

With this accountability guidance, Canadian Commissioners are raising the bar for what it means to be compliant. In a world of ubiquitous computing, big data analytics and cloud computing, it is not enough for a business to comply with the narrow letter of the law or technical provisions of the Act when a new tool or technology is introduced.

In an accountability framework, legal compliance involves a foundational commitment to privacy, and a deliberate and meaningful investment to build a living and breathing privacy model that has the flexibility to address new technologies, and the ability to comprehensively reduce the risk of costly privacy breaches, data spills and accidents.

Since the guidance document was published, we have begun to see accountability being implemented on a proactive basis as well as in response to some of our targeted work in specific sectors.

We've seen examples across health care, professional regulatory agencies, universities and government-owned corporations.

This guidance tool has put Canada in the global spotlight as part of the conversation on accountability. This Committee has an opportunity to take this work to its next logical step – express legal requirements spelled out in law that make clear what companies need to do in order to effectively protect the privacy of individuals.

This would be consistent with the revised OECD guidelines, adopted in 2013, which state that organizations should have privacy management programs in place and details what they should include.

I have provided additional detail in my written submission about how B.C. could follow suit and include express written requirements for accountability into PIPA.

I strongly recommend that the Committee consider how PIPA can be amended to more explicitly set out elements of a privacy management program that will assist organizations and individuals to ensure greater accountability.

ENSURING THAT THIRD-PARTY PROCESSING AND SERVICES ARE SECURE

One very important element of any privacy management program, especially in light of the numerous technological changes that have taken place over the last decade, is the responsibility organizations have to protect data when it is in the hands of third parties.

Here I am talking about technologies like the cloud, and other outsourcing tools used by organizations to store and process personal information.

It is often said that data knows no borders.

A business on Granville Street in Vancouver may be using a service provider that stores personal information on the other side of the world.

As it is currently worded, PIPA requires that businesses make reasonable security arrangements for the personal information under its control, including information that is not in the custody of the organization.

My expectation is that the same standard of security should apply to that data regardless of whether it is in a filing cabinet at the business headquarters on Granville Street or whether it's housed in the cloud and stored in Oklahoma.

However, this principle is not set out explicitly in PIPA. Adding such a provision will make the legal requirement crystal clear.

We have a good model in Canada's federal legislation PIPEDA, which is the language upon which I have based my recommendation to the Committee.

ACCOUNTABILITY – MANDATORY BREACH NOTIFICATION

Of course, accountability is about more than technical mechanisms for compliance. It is also about making sure that information is open, transparent and accessible in terms of an organization's privacy practices.

Individuals that hand over sensitive personal information in the course of doing business, deserve to know not only that an organization is properly managing that information – they should also know if that information has been disclosed, or gone astray.

Which is why breach notification is an essential part of a privacy management program.

This was one of my key recommendations when I appeared before the Committee last May. And I maintain that a legislated duty to report significant breaches is a critically necessary amendment to PIPA.

News articles about privacy breaches often focus on the numbers – the millions of dollars of direct and indirect costs to the company, or the tens of thousands of credit card numbers or email addresses lost.

Privacy breaches also carry a human cost. They put individuals at risk for identity theft and serious reputational harms not to mention loss of confidence, trust, and human dignity.

Breach notification would give those individuals an opportunity to be made AWARE of those real and significant harms, and take steps to mitigate them. And it gives them the choice as to whether they want to keep doing business with the organization in the wake of the breach.

Breach notification provides an important accountability lever in the business-consumer relationship.

The notification requirement would also extend to my Office, providing an important accountability mechanism from business-to-regulator. I believe making breach notification mandatory would provide an important and critical incentive for businesses to make the investment in privacy protection such that they could prevent breaches before they occur.

BC would **not** be charting new waters with such a provision; we would be keeping up with our trading partners. Almost all of the US states have mandatory breach notification and Europe is currently reforming its data protection framework that would make breach notification mandatory.

Our neighbours in Alberta have had a breach notification regime since 2010, and Bill S-4, the *Digital Privacy Act*, currently before Parliament in Ottawa could bring mandatory breach notification to the private sector federally very soon.

It is critically important that British Columbia's requirements be harmonized with those contained in the proposed federal legislation and with Alberta.

My understanding is that S-4 has already been through the Senate and started being studied in committee in the House of Commons. If it passes with the inclusion of mandatory breach notification, it will have a significant bearing on PIPA's "substantially similar" status under PIPEDA. Let me explain briefly what this means and how it is significant.

Back in 2004, when B.C.'s legislation first came into force the federal Cabinet declared PIPA to be "substantially similar" to the federal *Personal Information Protection and Electronic Documents Act*. This meant that PIPA, and not PIPEDA applied to the private sector in BC.

If we do not adopt similar reforms in our legislation, we could be putting our "substantially similar" designation at risk, meaning that companies would then be subject to two different laws (PIPEDA and PIPA) depending on the customer/employee context, and subject to two regulators. This would increase the regulatory burden on BC organizations.

For this reason, I am recommending that BC adopt mandatory breach notification amendments that are in line with those outlined in Bill S-4.

DISCLOSURES WITHOUT CONSENT / SPENCER

Just before moving to your questions, I would like to touch on one more matter that has arisen since my appearance before the PIPA Review Committee last May. That matter concerns section 18(1)(j) of PIPA.

A number of submissions to the Committee have commented on this provision in light of a Supreme Court of Canada decision.

Section 18(1)(i) of PIPA authorizes an organization to disclose personal information for the purpose of complying with a subpoena, warrant or order made by a court. In addition, an organization may disclose personal information to a law enforcement agency without a warrant under section 18(1)(j).

It is my view that what *Spencer* effectively does is clarify the range of disclosures permitted in section 18(1)(j). In *Spencer*, the Supreme Court of Canada made it clear that warrantless disclosures that are solicited by law enforcement are unconstitutional.

This decision dealt with a section of PIPEDA that is directly analogous to section 18 of PIPA. When law enforcement seeks voluntary disclosures from an organization the Court will now likely be treating them as unconstitutional searches of personal information, resulting in the information being inadmissible in court.

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

Amending section 18(1)(j) to limit it to organization-initiated complaints will bring it in line with the Supreme Court decision in *Spencer*.

That said, it remains very concerning to me that my Office still has no way of knowing the extent to which these disclosures may be happening.

For this reason I am also recommending that organizations in BC should be required to publish transparency reports on disclosures that are made without consent.

CONCLUSION

In closing, my key message is that PIPA is a law that was very current 10 years ago, but needs to be updated due to external changes, primarily flowing from technological developments with respect to use of personal information and from legal decisions.

Accountability and transparency provisions embedded in a privacy management program approach are key elements of our suggestions.

I would like to thank you for the opportunity to present my recommendations. I am happy to address any questions you may have.