OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

CHECK AGAINST DELIVERY

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

September 16, 2020

Michael McEvoy
Information and Privacy Commissioner for British Columbia

Good morning, Honourable Chair and members of the Committee. First, I'd like to respectfully acknowledge that we are located on the traditional territories of the Lək̓ʷəŋiṅəŋ people, also known as the Songhees and Esquimalt First Nations. Of course, we acknowledge all First Nations across the province who our office serves.

It is again my honour to appear before you to present my office's recommendations for reform of the *Personal Information Protection Act*. With me today are Deputy Commissioners oline Twiss and Jeannette Van Den Bulk.

I begin by expressing my gratitude for this work you have undertaken on behalf of British Columbians. The submissions you received in response to your broad and effective call for input highlight the urgency of that work. They clearly demonstrate that people and organizations in BC care deeply about privacy issues – and the rules that govern them.

Two themes can be discerned from many of those submissions; first, there is an urgent need to act on PIPA reform and second that those changes be, to the greatest extent possible, harmonized with standard developing provincially, nationally, and internationally.

Those submissions you have solicited also contain the answer to the question of whether PIPA reform really matters. What can be distilled is that reform matters because citizens expect government to protect privacy through meaningful legislated protections.

Evidence is to be found in the public opinion survey cited by the BC Freedom of Information and Privacy Association submission. The survey shows that more than two thirds of British Columbians feel they have little to no control over how their personal information is handled by the organizations they do business with, and only 43% of respondents feel that existing laws and organizational practices provide sufficient protection of their personal information.

Reform of PIPA **also** matters because modern privacy laws are key to maintaining BC's flourishing digital economy. British Columbia's technology sector generates revenues of $15.7 billion annually, accounting for 7% of our GDP and employing 114,000 people.

A digital economy can only flourish if individuals trust that their personal information will be collected, used, and disclosed within a framework of robust yet balanced privacy protections. If people lose confidence that their privacy will be meaningfully protected, they may well cease to allow their information to be used – or be reluctant to use digital services at all.

That is why, I think, many digital entities, like Canada's Digital Supercluster, support modernizing privacy laws… laws that strike the balance between use of digital technologies and privacy protection.

And given that data knows no borders, it is also imperative that the recommendations you make to change PIPA recognize standards developing nationally and internationally.

….

Should the Special Committee choose to endorse reforms to PIPA, our submission to you recommends that those changes address three broad categories:

1. the privacy obligations of organizations;
2. the privacy rights of individuals;
   and finally, the
3. oversight authority of the Commissioner

This morning, I would like to highlight three of our recommendations that fit within these categories. The remainder of my office's many recommendations are contained in our written submission, which we have provided you separately. We also, in that written submission, offer comments on selected stakeholder submissions, which we trust you will find of assistance.

I begin with what is the most important change the Committee could recommend … Mandatory Breach Notification.

This was one of my key recommendations when I appeared before you in June.

Neither public nor business interests are served by BC's current inaction on this matter.
Simply but strongly stated, BC and PIPA have become outliers on this issue, both domestically and internationally.

Once Quebec's Bill 64 is enacted, PIPA will be the only one of Canada's general private sector privacy laws that does not require organizations to notify individuals whose personal information has been compromised by a privacy breach.

The GDPR across Europe requires it.
The UK's *Data Protection Act, 2018* requires it.
Every single US state now has a law requiring it.

Mandatory breach notification is especially important now. Organizations are increasingly deploying modern technologies to compile our personal information. This profiling can include very sensitive personal health information, information about ethnicity or race, information about opinions or political views, or financial, educational and employment status. All of this is often the product of AI or other data analytics.

Given the growing sensitivity of these volumes of personal information, privacy breaches can have very serious and widespread consequences. These range from the financial harm to individuals flowing from fraudulent misuse of someone's banking details to threats to personal safety where information about a vulnerable person's whereabouts is compromised.

Mandatory breach notification is universally recognized as having at least three main benefits.

First, it permits individuals who are notified about a breach to take steps to protect their interests. This can include monitoring personal financial accounts and credit history, cancelling credit cards, and changing passwords for various personal accounts.

Second, mandatory breach notification gives organizations a real incentive to invest in information security technologies and policies, to better protect personal information against compromise. Progressive BC organizations understand that mandatory breach notification will enhance consumer trust, particularly if their business operations extend beyond BC's borders.

And third, breach notification can help a regulator stay up to date on trends in risks to the security of personal information and in turn allow my office to focus our educational and guidance work.

I stress that it will be important to harmonize BC PIPA's breach notification rules with the PIPEDA and Alberta PIPA approach. Canadian businesses are often challenged by patchworks of rules across the country… and the costs of complying with different rules cannot be **overstated**.

If the reforms we establish do not reach the benchmarks across the country, we also put our "substantially similar" designation at risk. Companies **could** be subject to two different laws (PIPEDA and PIPA), leading to an increased regulatory burden.

Individuals too will have an interest in harmonized breach notification rules. Many breaches affect Canadians across multiple jurisdictions. Regardless of where a breach originates, individuals are entitled to be notified under similar rules.

I note that PIPA should not require organizations to give notice of all breaches, only those where there is a "real risk of significant harm" to an individual. This is the approach taken by both Alberta and the federal government – and it is the one I recommend for BC's PIPA.

Taking again from both of these jurisdictions, I am recommending that PIPA require organizations to notify both affected individuals and my office of a breach. PIPA should also authorize my office to require an organization to give notice to affected individuals if that has not happened, including where we learn of the breach other than from the affected organization.

My office has long recommended mandatory breach notification, beginning with the first statutory review of PIPA in 2008, and then again in 2014. Both previous Special Committees recommended to the Legislative Assembly that PIPA be amended to include it.

I strongly urge you to do the same and I implore our legislators to act on your recommendations.

Consent

The second matter we draw to your attention today concerns the privacy rights of individuals. Individual privacy rights in PIPA are underpinned by the concept of consent. Many of the submissions you have received point to a pressing need to modernize consent requirements in the legislation.

I share that view.

PIPA's consent framework was born before Mark Zuckerberg dreamed up Facebook in his Harvard

dorm room… before Googling became a verb… and before the introduction of the iPhone.

Looking back, PIPA's consent provisions seem quaintly naïve in light of the ensuing avalanche of technological change.

Then and now, PIPA assumes that consent typically occurs in the context of a simple transaction between one organization and a single individual.
For example, you willingly give your name, phone number, and laundry to a dry cleaner with the understanding that your personal information is used for one purpose only – notification when your clothes are ready. If only all of our daily commercial interactions were still that simple!

But of course, they are not. Anyone who orders virtually anything online today will recognize this immediately. That concepts of consent are being contorted can be found on almost any website's privacy notice. They are often detailed, legalistic and in many instances remarkably **imprecise**– they leave individuals in the dark about how their personal information will be used and often obscure complex flows of data between various businesses.

They also frequently fail to disclose what technologies, including AI, might be used to process an individual's information – **and** what might be done with the resulting personal profile.

It is little wonder that we often click "I agree" without really knowing what we are agreeing to—or having much, if any, ability to do anything about it.

The complexity of these transactions highlights a need for legal reform that requires organizations to plainly state, in writing (I stress "in writing" because PIPA still allows notice to be delivered verbally) the intended use of the personal information they collect.

Quebec's Bill 64 is a good model, because it requires consent to be stated "in clear and simple language and separately from any other information provided to the person concerned." Bill 64 also obliges an organization, where asked, to provide "assistance…to help an individual to understand the scope of the consent requested." The essence of these changes should be to make consent **truly meaningful**.

However, even with clearly stated notice provisions, consent in today's world can represent nothing more than an illusion. Where large technology companies hold a quasi-monopoly position, people are often left with no choice but to accept whatever privacy terms are put before them. Given the reality of the power imbalance between individuals and large corporate actors and the "take-it-or-leave-it" attitude of many technology service firms, PIPA must go **beyond** consent reforms.

For this reason we make further recommendations to you in our written submission about automated decision-making, data analytics and profiling, data portability, and the right to be forgotten. Many of these recommendations are designed to redress the challenges the current digital ecosystem poses to the citizenry.

As I noted at the outset, our recommendations are aimed at modernizing organizational responsibilities, so that PIPA will both protect our citizens while creating a robust environment for innovative companies in British Columbia to thrive.

It has also become clear to me Madam Chair, that should the Special Committee advance recommendations to the Legislature along the lines we propose, these will only be meaningful, if they are appropriately backed up.

I have been a privacy sector privacy regulator inside and outside British Columbia. It is my considered view, and the opinion of many others, that PIPA is largely toothless when it comes to the enforcement of British Columbians' privacy rights.

As I noted in my initial presentation on June 2, 2020, our joint investigation reports with the Office of the Privacy Commissioner of Canada, including one involving the social media giant Facebook, exposed **the complete inadequacy** of PIPA when it comes to protecting the public's personal information.

PIPA is toothless because the most I can do to sanction even a serious, wilful violation of our legislation is to order an organization to do what it should have done in the first place—fulfil its legal duty under the law.

For this reason, the third recommendation that I bring to your attention this morning is a series of measures designed to strengthen the law's enforcement provisions. The first of these is the implementation of administrative monetary penalties.

British Columbians understand the evolving risks to their privacy flowing from technologies such as data analytics, AI, facial recognition, and more. **They rightly expect** that their privacy will be taken seriously and be backstopped by the same kinds of robust enforcement powers that exist in other areas, such as workplace health and safety and elections.

But they would be disappointed to learn this is not the case under PIPA.

As matters now stand, PIPA is devoid of any administrative financial penalties, even for the most egregious of offenders.

My office has always emphasised an educational and remedial approach to compliance with the law and we will continue to do so by working with organizations to secure compliance.

But the reality is that **some bad actors** will simply not honour their obligations under the law. This creates obvious harm for individuals whose privacy is at risk. It is also unfair to organizations who invest in the protection of the personal information they hold and who comply with the law.

What is needed is a flexible system of legal enforcement, that can in appropriate cases, impose monetary penalties on organizations that refuse to protect people's personal information. My office first called for this power to be included in PIPA in 2008.

Administrative monetary penalties are already commonplace across a range of regulatory fields in British Columbia. In addition to my role as Commissioner I also serve as the province's Lobbyist Registrar which, in appropriate cases, authorizes me to levy monetary penalties under the *Lobbyists Transparency Act*. Other examples include my colleague the Chief Electoral Officer, who administers a fine system under the *Election Act*, the BC Securities Commission, which can levy penalties under the *Securities Act*, and WorkSafeBC, which has that authority to do the same under the *Workers Compensation Act*.

Such powers are not new to privacy regulation in Canada. Ontario's Information and Privacy Commissioner has that power under the Ontario *Personal Health Information Protection Act*. The federal government is considering giving the federal Privacy Commissioner that authority under PIPEDA and as you know Quebec's Bill 64 proposes Quebec's privacy regulator be given extensive powers to administer monetary penalties. All of this follows developments in the UK, Europe and the United States.

And as our written submission to you sets out, it is not just a matter of administrative penalties. It is also important that my office's order-making power be reinforced by BC's courts in appropriate cases. This would bring PIPA into line with our Freedom of Information legislation which authorizes the filing of Commissioner orders with the Supreme Court of BC.

Other specific measures that will both enhance and clarify investigations and enforcement mechanisms under PIPA can be found in our more detailed written submission to you.

I remain firmly convinced that this modern suite of enforcement tools will be an indispensable instrument for protecting the personal information of British Columbians and serve as an incentive to organizations to make the appropriate investments in those same protections.

Conclusion

My message to you this morning is no more complicated than this; as law makers, as policy makers and as regulators, we need to work in tandem to keep up with the times. PIPA was drafted almost 20 years ago under very different conditions from those which we live under today. Rapidly evolving digital technologies, business models, and public attitudes toward privacy require us to respond in a way that is equal to the unique challenges we face.
Inaction is not a viable option.

To that end, our recommendations to you focus on legislative amendments that promote both protecting privacy and the importance of fostering innovation and investment in British Columbia's economic development… amendments that will allow us to keep pace with the rapidly expanding digital economy, **in harmony** with other jurisdictions, in Canada and around the globe.

I really strongly believe that this time really is different. The recommendations you make in response to this, the legislature's third PIPA review, will point the way forward for the protection of our citizens and enhancing our economic future in today's digital world. All British Columbians look forward to your report and to government's rapid, positive response to your recommendations.

I would like to thank you for the opportunity to present my office's recommendations. And now, I am happy to address any questions you may have and to ask you whether there is anything further my office can do to assist you in the work you have ahead of you.