OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

CHECK AGAINST DELIVERY

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

June 2, 2020
Michael McEvoy
Information and Privacy Commissioner for British Columbia

Good afternoon, Chair. Deputy Chair and Committee Members. Thank you for the invitation to address you this afternoon.

Joining me today are Deputy Commissioners Jeannette Van Den Bulk and oline Twiss.

Chair and Committee Members, as your province's access to information and privacy commissioner I have one task to accomplish this afternoon as you begin your important work to review the province's *Personal Information Protection Act*.

That task is to make clear that now is the time to reform BC's private sector privacy law. The BC government needs to clarify, strengthen, and enhance privacy protection to benefit both BC citizens and businesses.

The *Personal Information Protection Act* was once considered cutting edge. While its foundation remains strong, PIPA requires additions to bring it in line with modern standards of privacy protection.

Chair, as you observed, the COVID-19 pandemic has significantly changed how many of us work and communicate. The spread of the virus has also changed the way businesses

operate, schools run, and people practice their faith. We are, by necessity, full participants in a digital world.

As more of our personal information finds its way online, we need to know we can trust organizations to properly handle that information.
But the way personal information is collected and processed today is often outside the plain view of the individual or regulator.

As the Deputy Chair noted, artificial intelligence, a technology sustained by the harvesting of personal information, is advancing on a scale that could not have been imagined in 2003. AI operates in the shadows and includes algorithmic decision-making machines, datamining, data-matching and facial recognition… its use is pervasive and often opaque.

How can we as citizens trust these technologies and the companies that operate them to properly handle our personal information? It turns out – without proper regulation, we can't.

A single event with sweeping global implications drove that point home for both citizens and regulators. It is an event with which I am intimately familiar… because I was there.

… I led an investigation into this event.

Just over two years ago, I found myself in a cramped lawyer's office in London, England. I had been seconded, from my role here in BC as the OIPC's Deputy Commissioner, to the Information Commissioner`s Office in the United Kingdom, to help lead an investigation into how Britain's political parties handled the personal information of voters.

The project took a very different turn in that London law office. The UK Commissioner and I were invited to meet under a veil of confidentiality with a person we were told had worked for a certain company, then little-known, called Cambridge Analytica. I am not sure what I expected to hear on that grey January day.

But what transpired was truly shocking.…

This individual told a story of appalling abuse of personal data by Cambridge Analytica, aided by personal information supplied to it by tech giant Facebook.

We learned, among other things, how Cambridge Analytica extracted the psychological profiles of millions of Facebook users to weaponize targeted political messages.

The whistleblower who disclosed all of this to us is now well known to the world. His name is Christopher Wylie.

Our team at the ICO was the first regulatory or law enforcement authority to question Wylie. Weeks later, we were to discover the full extent of one of the world's most notorious data breaches.

We learned from Wylie that an app had been developed, called "thisisyourdigitallife," that allowed Cambridge Analytica to harvest the data of some 85 million global Facebook users, including 600,000 in Canada and 87,000 users in British Columbia.

The explosive story appeared two months later in the *New York Times* and *Guardian* newspapers.

It would have seismic implications for privacy around the world - including British Columbia.

Suddenly, people everywhere began to understand how their personal information could be exploited. The words "Facebook/Cambridge Analytica" became synonymous with what could go wrong when you share your personal information on a platform like Facebook. These intertwined names seared themselves on the public's consciousness, exposing what can happen with personal information when automated digital technologies rule.

The public began to ask: how could this happen? Were companies allowed to do this? What was government doing about it? And what were regulators doing about it?

When I returned home in late March 2018 to accept my appointment as BC's fourth Information and Privacy Commissioner, there was no escaping the fallout from the issues I investigated in the UK.

As it turns out, there was a deep connection to Canada and BC.

In a strange twist of fate, the whistleblower, Christopher Wylie, hailed from Victoria.

And there was another BC connection: AggregateIQ Data Services, the company that helped weaponize the Facebook data on behalf of Cambridge Analytica`s parent company, SCL Elections, was also based here in Victoria.

It became immediately clear to me and my federal counterpart, Privacy Commissioner Daniel Therrien, that coordinated regulatory action on the Canadian front would be required. We joined forces to look at both the Facebook/Cambridge Analytica breach and the activities of AIQ.

We found that Facebook did little to ensure its that the data of its Canadian users was properly protected.

Its privacy protection program was, in our words, an “empty shell.”

We also found that Facebook failed to properly audit many of the apps that were given access to its user data.

In the case of AIQ, we found, among other things, the company had developed “Project Ripon,” an architecture designed to make usable all of the personal data harvested by Cambridge Analytica.

None of the people whose data was taken and manipulated had given their consent.

Our joint investigation reports on Facebook and AIQ determined that the companies’ actions were contrary to BC and Canadian privacy laws.

Both Commissioner Therrien and I were asked in the wake of our findings, “What penalties could be imposed on these companies?”

The answer exposed the complete inadequacy of Canadian and British Columbia privacy laws when it comes to protecting the public’s personal information.

The total administrative penalty I could issue was… zero.

The same held true for the federal Privacy Commissioner, whose authority extends to provinces outside of BC, Alberta, and Quebec.

How can this be acceptable today, when the public expects us to hold organizations accountable for the collection and use of their personal information?

Meanwhile, we cannot ignore the fact that the rest of the world has moved ahead of BC and Canada.

In 2018, the British Parliament, recognising the inadequacy of its own administrative monetary penalty system in the wake of the Facebook investigation, adopted the General Data Privacy Regulation (GDPR).

The GDPR's fining authority allows for a penalty of up to 4% of a company's annual global turnover. But the GDPR sets outs a standard that is not just about fines.

The GDPR provides for a much higher level of privacy protection than what existed previously. It has gained recognition as the gold standard globally and has become the model for a number of national laws outside the European Union.

We in BC must be cognizant of these higher protections because our trade with European countries is closely tied to whether Canada's personal data protection laws meet the adequacy requirements under the GDPR. Without an adequacy determination, BC businesses are at a competitive disadvantage.

PIPA was a somewhat state of the art legislation upon its enactment in 2003. But in 2020, that is no longer the case.

We must get our house in order.

To put matters into perspective, when PIPA was enacted almost 20 years ago, Mark Zuckerberg had not even started to write the computer code for what would become Facebook.

Since then, the world of personal information collection and use has exploded. And if there was any doubt about the digital world's impact on everyday society, we need look no further, as you have said, Chair, than the events that have transpired during the COVID-19 epidemic.

How does the *Personal Information Protection Act* confront these challenges?

To return to the house metaphor, PIPA is a relatively new construction. It has a sound foundation and a good basic structure. But over the past 17 years its interior has experienced a lot of activity by individuals and organizations alike. What may not be so obvious from curbside is that the original builders left several major rooms unfinished.

Time moves on, but you never quite get to finishing those rooms. And day after day, you realize the limits of the dwelling's functionality.

This, I submit to you Chair and Committee, is your challenge – to complete the parts of PIPA that are incomplete.

PIPA's foundation, which is strong, rests on two pillars.

The first pillar is consent. With limited exceptions, organizations require and should continue to require consent of individuals before collecting and using their data. Ensuring that consent is meaningful is a challenge, especially in the digital world. I expect that over the course of your deliberations you may hear more about this and the need to enhance the consent provisions of the Act.

PIPA's principal-based approach of consent, modified in part for employment situations and a handful of other exceptions, means its structure is flexible and can be adapted to changing technologies. This is certainly one of PIPA's strengths; it doesn't have to be amended every time a new kind of technology is developed.

The other foundational pillar of PIPA is its recognition that organizations need to collect, use, and disclose personal information for purposes, as the statute states, "a reasonable person would consider appropriate in the circumstances."

This gives plenty of room for BC businesses to collect and use personal information in ways that can drive innovation in BC's economy and, in particular, the tech sector.

We are fortunate in this province to have a burgeoning tech sector. It is spreading its wings, not only in the Lower Mainland and on Southern Vancouver Island but also in places like Kamloops and Kelowna.

I have spoken with a number of businesses and entrepreneurs who understand the important value of privacy and the bond of trust it creates with customers and clients. They want to do the right thing when it comes to privacy, and our Office continues to provide guidance wherever we are able to assist organizations to implement scalable privacy management programs.

To that point: when the GDPR passed into law in Europe in May 2018, a number of BC and Canadian businesses revised their privacy policies to more closely align with what is considered to be the world's benchmark for data protection.

Business and citizens are ready for change.

They want and deserve laws that better protect personal information.

… legislative changes that will give greater confidence for consumers and organizations in everything from digital commerce and bricks and mortar services to social media and charitable gift giving.

So, what changes does this unfinished house of PIPA require? I expect your consultations will generate a number of proposals.

We will also provide our own detailed work plan in the weeks to come.

For now, I will focus on one room that needs to be finished… and one way to solidify PIPA's foundation.

I am referring to perhaps the most desperately needed addition to the house -- mandatory breach notification.

Privacy breaches happen when the security safeguards that an organization puts in place to protect the personal information in its custody or control are violated.

Breaches expose British Columbians to identity theft, financial harm, and reputational harm.

Yet in British Columbia in 2020 there is no legal requirement that an organization report a significant breach to my office or to those individuals exposed to a significant risk of harm.

This is not acceptable.

Further context is of assistance. We are witnessing a dramatic increase in the number and magnitude of privacy breaches in the private sector in this country.

Based on his examination of this issue, my colleague, the federal Privacy Commissioner, estimates that 28 million Canadians were affected by a privacy breach in 2018 – approximately 70 percent of our population.

When our Office last appeared before the Committee to review PIPA in 2014, we told members about a breach of highly sensitive personal health information by a testing laboratory in Kamloops.

That breach affected more than 16,000 British Columbians.

Five years later, in December 2019, the very same company revealed that its computer system had suffered a cyberattack involving the personal health information of 15 million Canadians – including five million British Columbians.

That company was LifeLabs. LifeLabs is now the subject of a complex investigation by my Office.

Chair and Committee members, my Office has reached the limits of what we can do to tackle this critical issue:

- We have stressed the importance of Privacy Management Programs for organizations.
- We have provided timely guidance documents.
- We targeted organizations with a year-long educational program called PrivacyRight.
- And we've made scores of presentations to organizations, including small and large businesses, not for profits, political parties, and more.

Our efforts at education and outreach are not enough to protect British Columbians especially as the digital economy expands.

PIPA stands almost alone in North America in its lack of mandatory breach notification provisions.

Both Alberta and federal private sector privacy laws were amended to require organizations to notify Commissioners of significant privacy breaches.

Mandatory breach notification exists in nearly every state in the US. It is also included in the GDPR and many other jurisdictions across the globe.

It is absolutely critical that organizations be required to tell individuals and regulators when a privacy breach could cause a real risk of significant harm.

We now receive voluntary reports of breaches both by public bodies and private organizations. This is good practice, but it represents only the tip of the privacy breach iceberg.

When those breach reports come to us we see our main task as helping the organization; helping them stop the breach and notify affected individuals when necessary. We also look at the organization's privacy management programs to see where they can be improved.

In some cases, we see privacy and security policies that are, to be blunt, appalling. But what are the consequences for an organization failing to report a breach or failing to invest in the protection of the personal information it holds?

Beyond an admonition from my office, effectively there is none.

We must create an incentive for companies to invest in the privacy and security of people's personal information.

It is, for this reason, necessary to legislate more than mandatory breach notification alone. Simply naming and shaming organizations will not bring compliance.

It would be as if you installed a state-of-the-art alarm system in your home, but when the alarm goes off, there is no response from the authorities.

To be effective, mandatory breach notification must be backed by the ability to levy administrative monetary penalties.

Fines are needed to incentivize compliance.

Administrative monetary penalties, or AMPs, change the calculus of how organizations think about their investments in proper security and privacy.

AMPs pair reputational damage with a serious financial penalty.

Or, framed in a more positive light, AMPs create the incentive to do the right thing.

A recent survey by the federal Privacy Commissioner's Office found that seven in ten Canadians would be more willing to do business with a company if it faced the threat of heavy fines for misusing their data.

It is clear that a fair and robust regulatory regime is good for citizens and for business confidence.

Conclusion

Trust is the currency that underlies all transactions involving personal information between people and organizations. The changes proposed to PIPA that we have touched on today, and will further detail in the weeks to come, will help build that trust. They will ultimately serve the public interest and that of all BC organizations.

When the Legislature built PIPA from the ground up in 2003, we were recognized as a Canadian leader in personal information protection.

With your guidance, we can lead again.

We hope that your work will not end with the issuance of your report.

Should you also come to the view that the house requires completion, I ask that you continue to champion your blueprint for PIPA's unfinished rooms with the executive branch of government.

This Committee's work could not have come at a more critical juncture. The serious need for privacy reform has only been amplified by the pandemic we are all living through.

We have provided our initial written submission and look forward to participating in the entire consultation process and providing additional detailed submissions as the Committee’s work unfolds.

Thank you again for undertaking the important task you have embarked on. And thank you once again for the opportunity to appear before you.

I would now be happy to respond to any questions you might have.