OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

CHECK AGAINST DELIVERY

SPEECH TO THE
BC FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ASSOCIATION INFOSUMMIT

September 30, 2020

Michael McEvoy
Information and Privacy Commissioner for British Columbia

Good afternoon, and thank you, Mike, for the introduction and your kind invitation to speak at this event.

Before I begin, I would like to respectfully acknowledge that I present to you today on the traditional territories of the Lək^{w} əŋiṅəŋ people, also known as the Songhees and Esquimalt First Nations.

I also want to acknowledge FIPA's service to the people of BC. The work that you, Jason, and the entire team does, adds immeasurably to public discourse in this province on matters vital to our democracy.

I want to spend the limited time I have this lunch hour with you focusing on the theme chosen for this conference: trust through transparency.

I think those words are more relevant than ever given that we find ourselves in the middle of a global pandemic affecting almost every facet of our lives… the adoption of digital technologies, including remote work, distance learning, and virtual health care, has accelerated rapidly.

Even this conference of course is being held in a new, digital-only manner.

It's sometimes hard to remember what the world was like pre-COVID… so much has transpired in the last six months.

What hasn't changed, however, is the need for robust access and privacy rights. In fact, their importance has been magnified by our current health crisis.

Before jumping into more detail on that topic: a brief refresher on the legislation my office oversees.

The *Freedom of Information and Protection of Privacy Act* (FIPPA) was brought into force in 1993. On the privacy side of things, FIPPA sets out requirements for public bodies in dealing with your personal information.

The law's essence is that public bodies can't arbitrarily collect whatever they want about you. They can collect your personal information if authorized by some law or regulation, or if it is otherwise necessary for carrying out their activities or programs. So, for example, turning over certain personal information would be necessary to get your driver`s license.

Sometimes there is a challenge to the authority of government to collect information, as was the case last year with the BC speculation tax, when it wanted to collect your social insurance number.

Ultimately my office ruled that your SIN is in fact necessary to reliably establish an accurate link between a land title holding and a tax return in order to carry out government's tax objectives.

FIPPA, of course, also establishes an individual's right to access records, including your own personal information, from a public body with certain exceptions; most people will know my strong view that the breadth of those exceptions has unduly widened in the last 25 years.

So that's the essence of the law as concerns public sector.

Personal information in the private and non-profit sector is dealt with under the *Personal Information Protection Act* (or PIPA). You have the right to access your own personal information under PIPA but as importantly the legislation puts limits on how organizations collect and use it.

Both FIPPA and PIPA, especially on the privacy side of things, play a critical and direct role in the everyday transactions we undertake as citizens, clients, or customers.

And what both pieces of legislation *really* attempt to underpin with regard to those transactions is **trust**.

Trust through transparency is the key to giving all of us the confidence to engage in a multitude of platforms. And one thing is clear in the face of COVID: there has been a massive explosion of digital platforms.

Contact tracing apps are perhaps most symbolic of the intersection between COVID 19 and technology. There has been a push for a Canada-wide contact tracing app, downloadable to your phone, that could potentially help to trace those people who might have been exposed to the virus. The Prime Minister recently restated his call for Canadians to download it as a means of fighting the pandemic.

The download and use of the app is of course voluntary here in Canada and many places around the world. A great many global public health officials believe the only way such an app can succeed in fighting the virus is if it is downloaded by many people.

For that to happen, British Columbians and Canadians, and here are those words again, will have to, collectively, **trust the app**.

In places like Singapore and – closer to home – Alberta, New Brunswick, Newfoundland and Labrador, Saskatchewan, and Ontario, the app has been made voluntarily available for download. However, people have shown nowhere near the kind of embrace required to make it practically useful to assist in flattening the virus's curve.

Since the outbreak of COVID-19, my office has been in contact with Provincial Health Officer Dr. Bonnie Henry and her team to discuss a contact tracing app as well as a range of issues related to information sharing and its potential privacy implications. These communications will continue as Dr. Henry and her colleagues lead the province's public health response.

From the outset of the pandemic, I have been clear that FIPPA and PIPA are designed to facilitate the **sharing** of personal information necessary to ensure the public's health and safety – to ensure that access to necessary information is available to those who need it – but not beyond what is necessary.

Since the outbreak of the pandemic my office has exercised our oversight and guidance role on a number of fronts with the provincial government as they have moved to implement measures to deal with the pandemic. For example, government consulted my office about Ministerial Order 085, an order temporarily lifting BC's data residency requirements.

Among other things, the order broadens the use of communication tools used by public bodies adapting to COVID-19. It allows health care bodies and workers to use technologies that may be hosted outside Canada to communicate and collaborate for the purpose of continuing service delivery during the public health emergency.

The temporary provisions of the Ministerial Order are, in my view, tailored and reasonable, given the challenging circumstances we find ourselves in. The technology tools allowed by the order, often referred to as third party applications, can only be relied on if they support recommendations or requirements related to minimizing the transmission of COVID-19.
It is important to remember that Ministerial Order 085 and succeeding orders do not give public bodies a free pass to ignore legal imperatives like proper security measures. It is also important to note that the order has a defined end date: it terminates on December 31, 2020.

One area that Ministerial Order 085 directly impacts is education and, in particular, K-12 education. The order does permit the use of a wider range of technology tools for distance learning in cases where students are not able to connect physically in a classroom.

This poses considerable challenges and is an issue that has been on our office's radar for some time, even before the pandemic. My office has been working with school districts and the BC Teachers' Federation to ensure e-learning can happen in a privacy protective way. And I should note that this is an issue that is not unique to BC; it has come up in many discussions with our provincial counterparts as well as international colleagues as part of our work with the Asia Pacific Privacy Authorities.

I also want to acknowledge the work done in this space by Mike and Jason and BC FIPA on this front and the contribution it has made to this discussion. I understand that the recent release of the FIPA report on gaps affecting privacy protection in BC's K-12 education system will be the subject of discussions tomorrow; we will be listening intently to that conversation.

COVID has also absolutely increased the velocity of developing societal trends on many fronts, including distance learning, as I just referenced, to the vast number of people now working remotely. My office has responded quickly to these shifts, answering many queries directly from the public and organizations and issuing guidance to assist individuals, public bodies, and businesses.

All of this ongoing oversight and our public education work I believe plays an important role in building public **trust** in the efforts to combat the virus.

In normal times, but perhaps more so in a public health crisis, government accountability is not only about the protection of personal information; it is also about the public's right to access information. Access to information is a critical part of our democracy and necessary to holding governments to account – even more so when the same governments are exercising extraordinary powers.

That said, the operations of many public bodies, especially smaller ones, were significantly affected at the outset of the virus' spread. For that reason, I proactively made a decision on March 18 that recognized both the challenges public bodies face in reorganizing themselves in the face of COVID-19 and the continuing need for accountability and transparency.
In that decision, I granted a 30-day time extension to public bodies to respond to freedom of information requests because, as I am authorized to do under FIPPA, I considered it fair and reasonable in the circumstances. I extended that order for an additional 15 days to give public bodies the time to arrange their operations to meet the provisions of the statute. Now that this decision has expired, and subject to particular circumstances, I expect them to meet the timeliness obligations outlined in FIPPA.

While I have just talked about the distinctive importance of the protection of personal information and access to information there are times when these two important rights intersect. Two recent examples come to mind.

I would first draw your attention to the recent report issued by my colleague, the BC Human Rights Commissioner. This report concerned the collection of what is termed disaggregated race-based data. The report highlights that caution is required in accessing personal information to advance laudable policy goals. A new statute governing the use of such data that is not addressed in existing access and privacy legislation may be beneficial and I look forward to working with the Human Rights Commissioner and providing guidance to government on this important matter.

The second example arises from a recent s. 25 complaint made to my office from several BC First Nations. I have been asked to consider whether the Ministry of Health and certain other public bodies failed to comply with s. 25 of FIPPA by withholding information about presumptive or confirmed COVID-19 cases proximate to the Nations' rural Indigenous communities.

Section 25 of FIPPA, most of you will know, provides for the mandatory disclosure of information by a public body where there is an imminent risk of significant harm to the environment or the health and safety of the public or a group of people, or where disclosure is for any other reason in the public interest.

All I can say at this point is that I await receipt of the party's submissions, and once I have the opportunity to consider those, I will be issuing a public decision in due course.

Through all of my office's actions during the pandemic, whether decisions, supportive guidance, or other initiatives, we are sending a clear signal that we want to help individuals, public bodies, and organizations navigate these uncertain waters.

We have also been clear that the foundational principles of transparency and accountability that underlie our laws must continue to inform how organizations, public bodies, and the public navigate this crisis.
Now, as I have traditionally done in my previous InfoSummit presentations, I want to turn to the recent work of my office.
I want to highlight the release of two reports looking specifically at access issues facing public bodies.

In one instance, we investigated whether public bodies were meeting their obligations under s. 71 of FIPPA to make categories of records available without an access request. We selected 30 public bodies across BC for this review and asked them to provide us a list of established categories of records and examples of records within those categories.

The resulting assessment revealed that public bodies are taking an uneven and inconsistent approach to their s.71 obligations. While some were doing a good job, we found that many others have a lot more work to do.

Earlier this month, I also released my report card on how timely the provincial government is in responding to access to information requests.

The report covered a three-year period from April 1, 2017 to March 31, 2020. One the one hand, government's response times have generally improved since the previous report was released in 2017.

However, this progress was set against a backdrop of thousands of cases where government extended the time it took to answer access requests without any lawful basis under FIPPA.

This issue is not new to government. However, the trend is accelerating and action is needed to reverse course.

As I mention in the report, nothing less than a shift in government's mindset is required to enable that to happen.

What is on our office's agenda looking ahead?

The need for reform of both FIPPA and PIPA is uppermost on our minds. Both Acts undergo a mandatory legislative review every six years and we find ourselves in the midst of the PIPA review right now.

The Special Committee to Review PIPA was struck earlier in the year.

I have always emphasized that a key role of my office is providing education and guidance.
But guidance and education only get us so far – citizens need to know that their privacy rights are properly backed up with effective enforcement mechanisms. Reputable businesses also need to know that laws are in place that hold bad actors to account. Otherwise, we risk skewing the playing field and creating an environment that undermines **trust** for everyone.
One area of special concern is the dramatic increase in private sector privacy breaches. British Columbia now finds itself almost completely alone in Canada, the US and Europe in not having mandatory breach notification requirements.

To be blunt, British Columbia's laws have fallen badly behind those of the rest of the world.

The European Union with its General Data Protection Regulation, California in the United States, and even Quebec in Canada have surpassed us in creating environments of trust and transparency.

The legal privacy paralysis shrouding our province is generating a cloud of distrust that threatens to undermine both citizen and business confidence in our digital future.

The time for reform is now…

That responsibility, of course, is with the provincial government, whoever that may be after October 24.

They must develop a robust regulatory regime that addresses the power imbalance between you and organizations that control your personal information.

I want to extend my praise and thanks to Mike Larsen and Jason Woywada, who on behalf of FIPA, clearly and unequivocally underscored the need for privacy reform in BC.

Once the provincial election was called, the Special Committee was dissolved. However, I expect their good work completed to date will be handed on to the new committee shortly after the election.

2021 marks the year FIPPA will undergo its mandatory review.

I get one crack at this review process in my tenure as Commissioner, and I want make sure we get it right.

I am going to depend on many of you out there to help me do that.

I am now in the process of working with my team here at the OIPC to develop a plan to engage with a number of you who are subject matter experts on access to information.
Obviously, my office has its own list of reform items, but I need to test them with you. It's important that I understand from your perspective, and that of others, how the Act is or is not working… and the best ways to fix it.

To that end, we will work to set up virtual discussion groups to facilitate these objectives.
Working together I believe we can continue to foster a climate of transparency and trust on both the access and privacy fronts in British Columbia.

Thank you again Mike, and I turn things back to you now.

I am happy to entertain any questions that the audience may have.