OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

CHECK AGAINST DELIVERY

SPEECH TO THE
SPECIAL COMMITTEE TO REVIEW THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

February 3, 2022

Michael McEvoy
Information and Privacy Commissioner for British Columbia

Good afternoon, Chair and members of the Committee. I would like to begin by first respectfully acknowledging that I present to you today on the traditional territories of the Lək̓ʷəŋiṅəŋ people, of the Songhees and Esquimalt First Nations.

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

It is my honour to appear this afternoon to provide this first, general briefing as you undertake the important work of reviewing British Columbia's access and privacy legislation.

Let me begin by addressing an elephant of some size occupying the room with us today, and here I speak of the role of this Committee in the wake of the amendments to the legislation that were just passed a few months ago.

In my letter of last October to the Minister responsible for carriage of those amendments, I described it as baffling that those changes would proceed in advance of your Committee having a chance to do its work. Some others wondered aloud what would be left for the Committee to do considering those changes, and if you did have recommendations to make about further reform, how those would be received by government.

To these matters I would say that, of course, I wished the government had allowed you to consider the changes proposed in Bill 22. However, there is still much work to be done — there remain significant matters unaddressed by the recent amendments that beckon this Committee's review and the government of British Columbia's consideration. I expect you will hear this from many others as well.

Those who know me, know that I am an ardent believer in our democratic institutions. Though I appreciate the healthy level of scepticism of government's future intentions in this realm, I believe that your work --- of consulting widely to gather information and encouraging fulsome public dialogue about proposed amendments -- is vital to advancing our province's access and privacy legislation.

The realist in me also thinks that if your work is to gain necessary traction, it will not end with the filing of your report. It will require that each Committee member use the knowledge gained from your consultations with British Columbians to persuade the government to advance the recommendations you put forward.

And as you undertake your critical work in considering what are sure to be many submissions, I wanted to offer you a way in which you might think about those suggestions; a lens, as it were, that may help guide your deliberations.

I think the most useful way to think about FIPPA is that it is a social contract between government and British Columbians.

On one side of the contract public bodies are permitted to collect information, much of it about us, so that it can function. That collection, amongst other things, allows government to provide important services or to plan public policy and programs.

On the other side of this bargain, British Columbians get an assurance that public bodies are accountable for the information they collect and use as well as being responsible for the protection of the personal information they gather about us.

In concrete terms, accountability is achieved through robust access to information where citizens have a window into what their public bodies are doing. Responsibility is achieved by ensuring there are proper guardrails around the use of personal information. Those guardrails must be reinforced by robust independent oversight.

In short, FIPPA is a contract with British Columbians in which government's authority to collect, use and disclose information is subject to pillars of accountability and responsibility.

I believe one of your most important considerations in undertaking the work ahead is to ensure the integrity of this social contract. This is especially so in an era of rapidly changing technology.

There is little doubt that these technologies have allowed ever increasing collection and processing of citizen personal information by public bodies.

To be clear, there are many benefits to society resulting from these advances. Accessing government services becomes easier and public policy and program planning can become a lot better. However, public trust and confidence in these systems, which is fundamental to their functioning, is only possible when citizens have a proper window into how government's business is being done.

As I just alluded, this trust and confidence comes through being able to readily access public body information, subject to certain exceptions of course, and to proper oversight of these matters by our independent office. Trust cannot be based on a one-way mirror where government knows and see a lot about us, but we can't see into its workings.

Where then, have the amendments in Bill 22 left us? Apart from the concerns I raised during the debate, I would say those amendments were focused on playing catch-up. Much needed reforms like mandatory breach notification and snooping offences, adopted in many other jurisdictions, finally gained traction here. Some other changes, like requirements for privacy management programs for public bodies, did bring BC forward and serve as an example of what legislators should strive for.

However, what the amendments *didn't* fully come to grips with are the advances in the data driven world we now live in fueled by a panoply of increasingly sophisticated technologies. What may constitute a record, for example, is a matter that might be something you wish to consider with a fresh lens given changes in information gathering technologies. To state the obvious, we no longer live in a paper-based world. Artificial intelligence, facial recognition technology, big data and data linking – these all impact our everyday lives, and FIPPA needs to do a better job of addressing them so that the added authority given to public bodies to collect and use data is matched by safeguards of oversight and transparency requirements.

I will have more to say about these matters in a few minutes but first, I know that you Chair, have asked through the Clerk of the Committee, that I spend some time today talking about the Act as it stands now, the work of my office, my perspective on the previous special committee's

recommendations from 2016. To that, as just noted, I will add some general observations about a potential way forward.

I want to start by giving a brief overview of FIPPA, about which you can find a more fulsome overview in my written submission.

The *Freedom of Information and Protection of Privacy Act*, has been in force for nearly 30 years now, since 1993. The purposes of the legislation are essentially threefold: to make public bodies more accountable to the public by providing a right of access to records (with certain exceptions); to protect personal privacy by setting out rules around the collection, use, and disclosure of personal information. The third purpose is embodied in my role as Commissioner, which is to administer the legislation by providing independent oversight of decisions made under it so as to ensure its purposes are achieved.

At this point it might be useful to give a brief history of the legislation. I feel like I have an intimate relationship with it, because as some of you may know, I was an advisor to the Attorney-General who piloted the original Bill through the Legislature - back in 1992. It was the first file assigned to me on taking my seat in an office just down the hallway from where we would have gathered this afternoon if an in-person meeting were possible.

The legislation had been long fought for by many people whose objective was to strengthen accountable government. When it was unanimously passed in 1992, FIPPA was considered state of the art legislation. It was a time, I need add, when most records to which the Act referred, were paper based - and email …. well Tom Hanks had then not even met Meg Ryan in the movie "You've Got Mail" for those of us of an age to remember such things.

FIPPA provides for government accountability by giving the public a right to seek records about what is happening in their community, how their tax dollars are being used, why decisions are made about their health care, and so much more.

This process is also an essential tool for members of this assembly, the media, and other organizations to get the information they need, to keep the public informed about how their tax dollars are spent and to hold public bodies accountable.

And, importantly, anyone can make an access request - and public bodies are required to assist them and to respond within established timelines.

As you know, access requests can be subject to fees. The first fee is an application fee that public bodies CAN charge, it is optional, and it is up to each public body to decide whether to do so. I continue to encourage ALL public bodies to forego charging their citizens a fee for making an access

to information request. I should also note that, unlike with other fees allowed under the legislation, I have no ability to consider whether such a fee should be waived in a specific circumstance.

The other type of fee that can be charged by a public body is for certain tasks associated with locating and producing records. This has been part of the legislation since inception and a public body can use their discretion not to charge or can excuse payment of this fee for a few reasons set out in the Act.

In terms of the public's right of access to records – it is not unlimited. Certain types of records are wholly exempt from an access request; for example, records that are already available for purchase, or more recently added to that list, certain types of records considered meta-data.

FIPPA also allows public bodies to withhold requested information in a record in certain circumstances. In some cases, a public body is actually required to withhold information - this would involve such matters as cabinet confidences and information which if disclosed would be harmful to business interests of a third party or to someone's personal privacy. In other cases, like with policy advice, withholding information on the part of the public body is discretionary.

These exceptions were initially crafted, I can attest, with some precision to ensure a fair and reasonable balance between the right of access and the need to protect certain information from disclosure. I think it also true to observe that the meaning of some exceptions has broadened considerably in light of certain court decisions. What is meant, for example, by the term "advice and recommendation" as an exception to disclosure under the FIPPA, is a good example of a term which has given wide berth to public bodies to withhold information.

While I appreciate, we mostly think about access to information in terms of what individuals request from public bodies, it must not be forgotten that FIPPA does not prevent public bodies from disclosing records *without* a request where those records do not contain personal information. In fact, I have, and continue to highly encourage public bodies to engage in this practice of proactive record disclosure, especially where it involves frequently asked for information. Not only does it encourage civic engagement and accountability, but it can also save a public body time from having to answer a formal access request on multiple occasions.

There is also a requirement for public bodies to disclose information, without delay, when the information is about a risk of significant harm to the environment or to the health and safety of the public or a group of people; or that, for any reason, is clearly in the public interest. When triggered, this mandatory disclosure under s. 25 of FIPPA overrides any other provision in the Act and so, as you might imagine, is generally triggered only in extraordinary circumstances.

A good example of s. 25's importance was revealed in our 2016 investigation into soil testing and water quality in the Township of Spallumcheen. We determined that it was absolutely critical, and clearly in the public interest, that the Ministry of Environment disclose information concerning soil testing because it had a direct impact on the safety of the community's drinking water.

I would now like to turn to the privacy side of FIPPA. The legislation sets out rules for the collection, use, and disclosure of personal information. Public bodies can only collect personal information when they have authority to do so and, in most cases, they are required to notify individuals about why they are collecting their information. Public bodies are allowed to disclose the information if doing so would be consistent with the original purpose for collection.

There are several other circumstances in which public bodies can collect, use or disclose personal information, many of which don't require the consent of the individual. These would include, for example disclosures for law enforcement purposes.

The right to collect your personal information also imposes on a public body the responsibility to properly secure and protect it. . The degree of that protection can depend on factors such as the sensitivity of the information and the potential for harm should it be disclosed without authority. A person's medical information will, as a general rule for example, require higher safeguards than a simple email address or first name.

And, in the event those safeguards fail, there will soon be a requirement for public bodies to notify my office, as well as affected individuals, of a privacy breach where it can reasonably be expected to result in significant harm. This means that not every single breach will need to come to my office. A single email that goes astray with little consequence, for example, will not need to be reported.

FIPPA also requires public bodies to use various tools and resources to meet their responsibility to protect privacy. For example, public bodies must conduct privacy impact assessments, or PIAs, to determine whether their proposed initiatives comply with the law.

Finally, I'll note that the recent amendments to FIPPA will require public bodies to develop privacy management programs, in accordance with the directions of the minister. This is something my office has long advocated for, and in fact issued guidance on back in 2013.

In my remarks this afternoon I have referred to some specific investigation and audit work we have accomplished. I now want to speak my Office's role in more general terms.

As I mentioned earlier on, I am responsible for monitoring how FIPPA is administered to ensure that its purposes are achieved.

In broad terms, it means I undertake investigations and audits, issue binding orders, engage in research, educate, and inform the public about FIPPA, as well as comment on the many different types of government initiatives as was the case with recently proposed legislative amendments.

Much of what we do, the meat and potatoes of our work so to speak, involves requests for reviews and complaints.

If a public body decides it's not going to release information in response to an access request because they say it is subject to an exception, like solicitor client privilege for example, the requestor can come to us to challenge that decision. Similarly, if a requestor is unsatisfied with the way a public body has handled a request because, let's say they have exceeded the time limit for a response, they can also complain to us.

To give you a better sense what this means, in the past fiscal year my office received approximately 885 requests for review and complaints about access requests.

Whether it is a request for review or a complaint, our case review team initially processes the matter and sometimes can quickly resolve it. If they can't, it will be assigned to one of our investigators who will attempt to resolve it informally, either by working with all parties to achieve consensus or by issuing findings. Mediating these issues can be challenging, because in many cases the parties before us have a strained relationship.

My case review and investigation teams are highly skilled and resolve most of these files something in the neighbourhood of 90% of them. In the proportionally small number of cases where that doesn't happen, the matter will proceed to a formal inquiry, where an adjudicator will make a binding order subject only to judicial review. I will note that the files that make their way to adjudication are typically complex and contentious matters, the majority of which are access requests.

I mentioned the adjudication process in my recent presentation to the Select Standing Committee on Finance and Government Services, and I do think it bears repeating that my Office's responsibility to interpret and apply FIPPA's meaning is critical to the Act's foundations. For the indigenous woman seeking records about her grandmother's incarceration in a juvenile reformatory in the 1940s to homeowners seeking local District government documents explaining geotechnical findings making their properties uninhabitable --- the issues at stake in these determinations can be far ranging and very significant for the individuals and communities involved.

My office also assists public bodies and organizations that have experienced a privacy breach. Last

year we received 92 privacy breach reports related to the work of public bodies. Our comprehensive response to these reports is to provide advice and guidance to public bodies involved and help to ensure citizens have the information needed to protect themselves against the fallout from the breach.

As a side note, we expect the number of breaches reported to our Office to significantly increase with the implementation of mandatory breach notification, and we are actively preparing for this on an operational level.

My Office also releases public reports throughout the year conducted by the audit and systemic investigations team. These are usually initiated either in response to a complaint or done proactively.

Our look at how the access to information system is faring during the COVID epidemic is a recent example. Others include our section 71 report, that looked at how public bodies establish categories of records available without an access to information request, and our routine report card on government's access to information timeliness.

We also teamed up with the BC Ombudsperson and the Yukon Ombudsperson and Privacy Commissioner to report out on the challenges to privacy and fairness arising from the use of artificial intelligence in the public sector. The recommendations in the report will, I believe, be of value to the work you are doing.

Finally, a very important part of my office's mandate is education and guidance. We often consult with public bodies seeking our comment on their proposed initiatives or questions. We also routinely release guidance documents for the public and public bodies alike, about the legislation and other relevant access and privacy issues. For example, we released information in September following the implementation of the BC vaccine card, to explain how the card, the Public Health Orders, and BC's privacy laws work together.

Collaboration with our counterparts, both across Canada and internationally, also supports our work, advancing our knowledge and expertise in access and privacy issues. We regularly collaborate with federal-provincial colleagues witness our recent joint statement respecting vaccine passports.

I am going to stop there on our Office's work because I know time is at a premium this afternoon. What I will do is point you to our written submission that expands on all these responsibilities.

I now want to briefly touch on recommendations made by the previous 2016 Special Committee. For ease of analysis, I have included an appendix in our written submission to you, with a table that shows where Bill 22 amendments addressed the 2016 recommendations.

When I say some Bill 22 amendments "addressed" the 2016 recommendations I do not mean to say that those recommendations were fully implemented in all cases.

For example, the previous Special Committee recommended extending coverage of the Act to what are often referred to as subsidiary corporations – organizations that in some instances carry out essentially government functions but avoid FIPPA accountability because they are not technically a public body. Bill 22 amendments expand the range of entities that the Minister can designate a public body but ultimately leaves it to her discretion to do so. In my view this fell short of the 2016 Special Committee recommendation which was to make such coverage automatic when certain criteria are met.

In general, I would say that the recent Bill 22 amendments more readily addressed the privacy, penalty and offence recommendations of the 2016 Committee, than those dealing with the improvement of access to information and information management.

With respect to the 2016 recommendations that were *not* addressed in any fashion by the government in Bill 22, I intend to address those in a detailed way in follow-up briefings to you, because I believe there are many that remain relevant and warrant further consideration by your Special Committee honourable Chair. On the access side, for example, you can expect I will be proposing recommendations that narrow the exceptions to disclosure that can be used to withhold information and to expand coverage of the Act.

I will also be monitoring the impact on public right of access to information by any public bodies who elect to charge a fee for their citizens to exercise their right. I hope to share some initial insight with you on that issue in the coming months and what that might mean to your recommendations to government.

In terms of privacy, I expect I will make recommendations to you on government use of automated processing and artificial intelligence. Closely related to this await I can advise the Committee that I eagerly await the draft set of rules for data linking which I understand the government is now drafting and about which they are required to consult me. Together, these matters carry both significant promise in terms of yielding insights and efficiencies but carry significant risks for the privacy of British Columbians.

As I mentioned, it is my job to monitor and enforce the Act to ensure that its purposes are achieved.

In that respect I observe that the powers of my Office have remained largely unchanged since FIPPA was introduced 30 years ago – even though access and privacy issues are only becoming more pronounced and consequential. Therefore, I will also bring forward recommendations that will both improve and streamline our processes, while providing stronger and more effective oversight.

In concluding my remarks this afternoon, I can do no better than restate the message I recently gave to the Special Committee to Review the Personal Information Protection Act, our private sector legislation,: as law makers, as policy makers and as regulators, we need to keep up with the times.

FIPPA was drafted 30 years ago under very different conditions from those which we live under today. And though, some elements of the legislation, including its core purposes, have stood the test of time, it behooves us to ensure that it adapts to modern challenges so that the citizens of our province are properly served.

I want to thank you for your work on behalf of the citizens of British Columbia and for the opportunity to appear before you today. I welcome your questions.