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

April 7, 2022

Michael McEvoy
Information and Privacy Commissioner for British Columbia

Good morning, Chair and members of the Committee. I would like to begin by first respectfully acknowledging the place from which I present to you today on the traditional territories of the Lək̓ʷəŋiṅəŋ people, of the Songhees and Esquimalt First Nations. I am grateful to live and work with people from across many traditional and unceded territories, covering all regions of British Columbia.

With me today are the OIPC's Deputy Commissioners Jeannette Van Den Bulk and oline Twiss.

I want to begin by thanking each of you for your work on this Committee. It is easy to be a skeptic or a cynic about the task you have been charged with. But the work of advancing the *Freedom of Information and Protection of Privacy Act* is critically important to serving the public interest.

We live in a democracy that we can be thankful for but too often take for granted. Fundamental to our system of democratic governance is its carefully calibrated system of balances and checks between citizens and those who make decisions on our behalf.

One aspect of this relationship is the huge mass of information public bodies acquire, both as a collateral aspect of governance and what is collected about us citizens - all of which is, for the most part both necessary and legitimate.

What is the check? Or the balance? An important part of that answer is the *Freedom of Information and Protection of Privacy Act*. It checks how public bodies collect and use personal information about us. And, just as important, it opens the door to the information associated with governing us; balanced of course by narrow exceptions to that right.

At least that is the way it should be.

What is clear is that the system of checks and balances has somewhat eroded with time. It reminds us that we cannot take this part of our democratic foundation for granted. It's why your work is important and why it matters.

My purpose in being here this morning is to follow-up on our general presentation to you in February and to provide you with a more detailed set of recommendations to fortify and advance the *Freedom of Information and Protection of Privacy Act*.

I was deeply impressed by many of the submissions made to you already by individuals, civil society groups, journalists, and others. If there were any doubt, it is abundantly clear that British Columbians care deeply about the legislation you are charged with reviewing.

What I will focus on today in my remarks are select recommendations found in my written submission provided to you. I will also address the questions posed by the Committee after my last presentation.

First, however I want to briefly comment on an issue not addressed in detail in my submission -- the new provision in FIPPA that allows public bodies to charge an application fee.

I want to reaffirm my office's intention to assess the impact of that fee on the public right of access to information. We will base that analysis on the six months of data marked from the start of the fee's imposition until May, and those findings will be made public.

I also want to reaffirm my strong encouragement to all public bodies to forego charging their citizens a fee that makes accessing their information more difficult. And I am pleased to see, for the most part, that appears to be the case.

I now turn to highlight recommendations provided to you in our written submission.

They are grouped into three categories, or themes, mirroring the structure and purpose of the legislation.

- Access and accountability;

- Protection of privacy; and
- Enhanced oversight.

I will focus on a few key recommendations in each category this morning. The remainder are found in our written submission provided to you, and which has been made available both on our website and the Committee's page.

Let me begin with perhaps one of the most important recommendations, both from a substantive and symbolic perspective. The issue is this -- the very Assembly that unanimously voted to pass FIPPA in 1992 failed to apply the law to itself. Somewhere in the mists of history we have lost account of why this happened. However, I do not think it a reach to suggest that if the law's sunshine had been shone on this institution since 1992, as it did with all other public bodies, we may not have endured controversies that have occasioned this institution in the time since.

And it was surely because of particularly recent events that the then and still Government House leader, the Honourable Mike Farnworth, agreed with recommendations put in a letter to the Legislative Assembly Management Committee in 2019 by me, the Ombudsperson, and the Merit Commissioner, that the administrative functions of the Assembly be covered by FIPPA. This commitment was subsequently reiterated in a meeting he had with the three of us.

There is simply no cogent reason the same rules that apply to more than 2,900 public bodies across the province should not extend to the Legislative Assembly. It expends public resources and performs a public function just like any other.

To be crystal clear, this change would not, and I cannot emphasize this strongly enough, would NOT impact the standing of the Legislature, impinge upon the legislative work of government, nor affect the constituency work of the Members of the Legislative Assembly.

The government has made a commitment on this important issue. The time is now to make good on this promise and I would strongly urge you to recommend the same in your report to the Assembly.

I mentioned at the outset about certain important checks in FIPPA having eroded. I will briefly highlight two that require your careful attention.

The first concerns s. 13 of the Act, whose evolution, resulting from various court decisions, have so seriously misshapen its meaning that the public's right of access to records has been significantly undermined.

Section 13 of FIPPA allows a public body to withhold information that would reveal "policy advice or recommendations." The purpose of the exception is to enable full and frank discussion of policy issues in the public service. However, what is now considered to be "advice or recommendations" that a public body can withhold from public release has gone far beyond what was intended by the Legislature in 1992. Specifically, advice and recommendations have been defined to include factual, investigative, or background material, including the assessment or analysis of such material, and professional or technical opinions.

At a time when disinformation runs rampant, facts are in short supply and the public struggles to understand those basic facts on which government makes its decisions – the letter and spirit of the Act and public trust in it are undermined when those basic facts giving rise to decisions are kept behind closed doors.

This recommendation – to affirm what Act's drafters intended, whereby factually material should not be withheld - has been advanced to and supported by past Special Committees which have considered the matter.

The second check sustaining erosion concerns not what the Legislative Assembly put in the Act, but what the courts have added to it. Section 14 of FIPPA is precisely and properly drafted to allow public bodies to protect privileged communications with their lawyers. That's it. No other kinds of privilege are included. By way of comparison, Alberta's Access legislation provides for both solicitor-client and something called settlement privilege as a basis for withholding information from a requestor. Our legislation was meant to provide public bodies and the public with a complete code of exceptions to disclosure. Settlement privilege was not included in FIPPA, but despite this, a court decision has, as we lawyers like to say, been read it into our Act. Which in plain language means it has been added to our legislation.

Why is this especially problematic? An important example will suffice. For many years, public bodies disclosed the payouts made in severance packages in response to access requests. This kind of information can shed considerable light on the administrative competence of our public bodies in addition to identifying the costs to the public purse. The payments may or may not be justified, but from a FIPPA point of view the public has a right to know about these kinds of often substantial public sector expenditures. Increasingly however public bodies are attempting to hide these payouts behind the curtain of settlement privilege.

FIPPA should be amended to make explicit that the list of exceptions to disclosure set out in the Act is exhaustive and does not include settlement privilege.

I mentioned grouping this morning's presentations into three categories or themes. The second is about the protection of our personal information. Recent changes to FIPPA made some positive

updates to the privacy rules designed to protect our personal information. Mandatory breach notification and a requirement that public bodies develop privacy management programs are good steps forward. But for the most part, these changes were a catch-up to reform recommendations made in other jurisdictions years ago.

The challenging task you face, I believe, is making recommendations that position FIPPA as a forward-looking statute that contemplates the technology - the use of which we are now beginning to consider and which we can expect will be - used increasingly in our digital society.

We absolutely want public bodies to innovate and use new technology to improve policy making and to find efficiencies to better serve citizens. However, if these advancements are to be embraced and trusted by the public they will need to protect and treat with respect British Columbian's personal information.

This means having clear and enforceable rules that place guardrails around the use of new technologies. One area in particular stands out -- automated decision-making and its companion, artificial intelligence.

Government makes decisions about all of us every day that may allow us to access health care or determine if we are eligible for social assistance. Increasingly these kinds of decisions will be made by automated means, and such systems will deploy so called artificial intelligence in making them. We as citizens may be the collective source of that artificial intelligence, in the sense that the vast reservoir of personal information government's holds about us will be processed to profile us, seek patterns, or insights into our behaviours as citizens, and to predict future outcomes.

All of this may yield considerable value to society. But it may not if used improperly.

This is what separates an automated decision-making system and use of artificial intelligence from other technological advancements that increase efficiency – it doesn't simply process information faster, it processes information *differently,* and in a way that is not always clear to those running the system, or to the individual affected by a resulting decision. In other words, you can be directly affected by the output of the system, but its so-called reasoning is unknown, perhaps even to the person running the system.

Because of this, specific measures are needed to ensure the responsible and fair use of these systems by public bodies. As it stands, s. 31 of FIPPA requires public bodies to retain information used to make a decision about an individual for at least one year. However, you can see how this is difficult when a public body can't determine *what* or how information was used to make the decision in question. While these systems may still be in the early stages we need to be prepared because Canada, in fact, is a global leader in AI. The regulation needs to be in place before we get

too far down the track because, and to mix too many metaphors, once the genie has left the bottle it may be too late.

Therefore, it is imperative that FIPPA be updated to grant individuals the right to be notified if an automated-decision system is being used to make a decision about them. Individuals should also have the right to receive a meaningful explanation of the reasons and criteria used to make that decision, and to object to the use of an automated-decision system.

We are also recommending that FIPPA require public bodies to create a traceable record of how a decision is made that impacts an individual using an automated decision-system. If an explanation cannot be provided, due to trade secrets or security classification, a public body should provide the individual with the type of personal information collected or used, why the information is relevant, and the likely impact on the individual.

The final category or theme I wanted to highlight for you this morning focuses on the very building blocks that support our legislation. I want to talk about those building blocks and why we need stronger oversight mechanisms to ensure those foundational footings are properly supported.

When I use the term building blocks I am really talking about the proper creation and retention of public body records. Without this there can be no meaningful access to information system.

A right of access to information depends on records being available in the first place. If records are not created, or if they can't be located and retrieved, or if they have been improperly destroyed, rights of access are fundamentally impaired.

Good public administration and governance cannot be achieved without proper record keeping systems. Tracking the life cycle of a record is critical to understanding how government runs and how its decisions are made.

It must also be remembered that those records that underpin the functioning of good government ultimately, in a collective sense, belong to the people of British Columbia and, with some exceptions, individuals in this province have a right of access to those records.
So, a question arises – if this system is so important, how do we ensure its building blocks are put in place, well maintained, and functioning to support proper public sector governance and access to information?

The answer is that government has begun this task - but it is far from complete.

A starting point can be found in the *Information Management Act,* which is something this Special Committee asked me about during our previous session. You asked to what extent the IMA has or

has not addressed the 2016 Special Committee's recommendations. I would agree with the assessment of the IMA offered by your predecessors on the 2016 Special Committee who rather tepidly described the IMA as a move in the right direction. It noted, among other things, it only applied to a limited number of government bodies. It strongly recommended that the duty to document decisions be put in FIPPA in order to ensure its broader application to all public bodies.

We agree with this recommendation and would go a step further.

A duty, including the duty to document, is of little value if it's not backed up. And this is a serious shortcoming of the IMA. In addition to its lack of breadth there are no mechanisms within it to ensure the proper record keeping required of Ministries is actually carried out.
At most the Chief Records Officer can review a government record management system and make a recommendation about it. That's the extent of it.

No power to require a ministry to do something, as a duty might imply. No sanctions available to the Chief Records Officer if, for example, an information schedule is violated or records are improperly destroyed. The system set up under the IMA can in no way be described as a robust or independent mechanism of oversight over our critical record management system.

This needs to be rectified.

I point to two measures that would begin to attend to these concerns. These are already found in other public sector privacy and access legislation in Canada.

First, freedom of information legislation in Ontario requires public bodies to have record keeping and retention rules and policies. This allows the Ontario Commissioner an overall independent window into government's management of records. A similar provision inserted into BC's FIPPA would do the same. It would not be aimed at my office micromanaging the disposition of individual records but rather it would give my office the ability to ensure that public bodies are attending to basic records management responsibilities, on which their work and the right of access relies.
The second measure is the independent oversight over allegations of the unauthorized destruction of records. This power is longstanding in Alberta, and has been used in that jurisdiction to, for example, investigate and alleviate concerns that a change in government lead to the widespread destruction of records.

I made this recommendation to the last Special Committee, and it accepted that recommendation.

Therefore, I am recommending that FIPPA require public bodies to have in place reasonable measures respecting record keeping and retention rules and policies. This would of course apply across all public bodies in line with the 2016 Special Committee recommendation. I am also

recommending that s. 42 expand the Commissioner's oversight by granting the Commissioner the jurisdiction to review matters or allegations of unauthorized destruction of records that occurs outside of or prior to an access request.

I believe this answers the question you posed to me at the conclusion of our previous appearance about the Information Management Act. The other question you asked concerned what public sector statutes in other jurisdictions can we look to as you undertake your deliberations.

You will note that in our written submission, we cite provisions from a number of other laws in Canada and abroad that offer greater protections and transparency, and that can serve as examples of what we should look to as we consider reform here in BC.

I just mentioned provisions related to information management found in the statutes of our counterparts in the provinces of Alberta and Ontario. The jurisdiction that most recently revised its legislation in a significant way is Newfoundland and Labrador. I would commend to you a provision there that requires public bodies to consult with the Commissioner on any proposed changes that affect access and privacy rights of citizens in that province.

Interestingly a similar requirement for consultation is found in Europe's General Data Protection Regulation that applies to public and private sector entities.

I cite here just some examples of course. We will chart our own made-in-BC solutions, but to the gist of your question, there certainly are things we can learn from jurisdictions both here in this country and abroad.

In concluding my remarks today, I return to observations I made in my first submission to you in February about how our Freedom of Information and Protection of Privacy legislation represents, in a very real sense, a social contract between citizens and our public bodies.

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.

I have also attempted to underscore how important this bargain is to our democratic system of governance in British Columbia. It adds a necessary set of checks and balances that supports our democratic infrastructure.

You have much to consider in taking account of all that you have heard from citizens during the course of your review.

Some have expressed frustration about how the legislation has changed and evolved over time, fraying that social contract and in some circumstances paring back the carefully calibrated checks and balances within it.

I share a number of those concerns and frustrations. Time has taken something of a toll on some of the provisions of the Freedom of Information and Protection of Privacy Act. But I also believe at its core the legislation is sound. That BC's access and privacy system is a good one and that it contributes in a fundamental and appreciable way to the democratic foundations of our province. But it can be even better.

I believe your work will go a long way to making it so. As you begin to craft your recommendations for government please know that my Office continues to be available to assist your deliberations in whatever way we can.

And with that, Chair and Members, 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.