CHECK AGAINST DELIVERY

SPEECH TO THE
SELECT STANDING COMMITTEE ON FINANCE & GOVERNMENT SERVICES
February 27, 2023

Michael McEvoy
INFORMATION AND PRIVACY COMMISSIONER/ REGISTRAR OF LOBBYISTS

Good evening, Honourable Chair, Deputy Chair, and Members of the Committee.

I would like to acknowledge that I present to you today on the traditional territories of the Lək̓ʷəŋiṅəŋ-speaking people, also known as the Songhees and Esquimalt First Nations. As an Officer of this Legislature I also acknowledge that I am privileged to work with people across many traditional territories, covering all regions of our Province.

Joining me this evening are Deputy Commissioners oline Twiss and Jeannette Van Den Bulk. Also here as always to assist is Dave Van Swieten, Executive Director of Shared Services, who serves in this capacity for the four Officers of the Legislature headquartered at 947 Fort Street here in the Province's capital.

I begin by thanking this Committee for recommending my 2023-24 budget request to government in October, and to say I very much appreciate the time afforded us this evening.

I promised the Committee last fall I would request this appearance once the government announced the date for implementing amendments to the *Freedom of Information and Protection of Privacy Act*, which add considerable responsibilities to my office.

Those amendments, announced in late November came into force just a few short weeks ago, February 1, and

they do two important things for British Columbians.

First, they require public bodies to notify affected people, and my office, of privacy breaches that could be expected to result in significant harm. This must be done without unreasonable delay. Second, public bodies must now develop privacy management programs.

Both measures are important steps in securing the personal information of British Columbians, and improve public body accountability.

My office is already stretched beyond current capacity, and we know the new mandatory requirements, especially those involving privacy breaches, will require a labour-intensive response if they are to be implemented in the manner the legislature intends. We know this from the small percentage of the province's 2,900 public bodies that already voluntarily report breaches to our office.

When such unauthorized disclosures are reported they require immediate attention. From a police officer's notebook left exposed --- to the medical clinic whose patient record system has been locked down because of a ransomware attack -- the stakes are high.

When our front-line staff are notified of a breach, they immediately assign a case review officer or investigator who in turn contacts the public body to monitor and guide them through the management of the unauthorized disclosure.

This involves a number of detailed steps, the first of which is to work with the public body to contain the breach. That is critical to limiting the severity and ultimate impact of any unauthorized disclosure.

That process works hand in hand with ensuring the details of the breach are thoroughly documented; fundamentally important to understanding who is affected by it, the number of affected individuals and the type of personal information involved.

All of this is necessary to evaluating the risk and foreseeable harms arising from the breach and contributes to a determination of whether there exists a risk of significant harm to an individual whose personal information has been breached.

Where this is the case it may be necessary to notify those individuals affected so that they may take steps to mitigate the harms. Who should be notified and the manner of notification will often be a matter of intensive discussion between a public body and our office.

In some cases, these discussions between my office and a public body will be clear and straight forward. In many cases they will not. Indeed, in many cases we expect public bodies will be reporting to us when they are not sure whether they need to; that is to say it will not be clear if the breach is likely to pose a risk of significant harm to an individual.

Particularly in the first few years of the law, I expect this to be the case as public bodies grapple with their new and important responsibilities. It may be, and this has been the experience elsewhere, that public bodies will have a tendency to over report breaches. This is in my view, not a bad thing. It is better to err on the protective

side of the decision spectrum.

Whether a public body is sure or unsure of their standing we will be there to help because that is what the public interest demands.

And ultimately, we will be there to ensure the root cause of the breach is determined so that steps can be taken to protect against future incidents.

All of this will require additional resources because, as I have noted, we already find ourselves operating at stretched capacity. We have turned to other jurisdictions that introduced mandatory breach notification to help us assess the additional pressures it will place on the work of our office.

This review disclosed that we will experience a jump in case files as we move from voluntary to mandatory breach reporting. The increases experienced by other jurisdictions have ranged from 50% in some instances to as high as 700% in others.

When Australia and the UK introduced mandatory breach notification in both the public and private sectors, the Privacy Commissioners in these offices saw a 300 and 700 percent increase in notifications respectively.

Manitoba introduced mandatory provisions for the public and private health sectors on at the beginning of 2022 and saw an immediate 50 percent increase in notifications, and those numbers continue to trend upward.

When Alberta brought mandatory breach notification to the health sector -- which is both public and private -- the Commissioner's office reported a four-fold increase in breach reports in year one, a six-fold increase in year two and now three years later they find themselves dealing with triple the reports they experienced prior to mandatory report.

Based on the experiences of our counterparts, our best estimate is that BC's new requirements will result in a 300 percent increase in breach notifications from public bodies.

Our colleagues also shared with us that in addition to the breach reports we should also brace for an increase in complaints about *whether* public bodies have responded to a breach appropriately. Such complaints could be about individuals who had their personal information compromised in a breach, or could be from individuals who weren't notified of a breach's occurrence.

This will in turn almost certainly lead to the need to conduct investigations or audits when we have reason to believe a public body has not complied with these new breach provisions in FIPPA.

And all the while it must be kept in mind that beyond legal compliance, my office has both a mandate and responsibility to support important educational work about the new requirements, raising awareness across all public bodies about their responsibilities. Ramping up those efforts will ensure public bodies are proactively managing personal information and privacy breaches.

*****

I will now shift to the other requirement that came into force on February 1: the obligation of public body heads to develop a privacy management program, in accordance with the Directions of the Minister. This requirement is also an important one: a privacy management program – or PMP as we call them - ensures that privacy is built into initiatives, programs, or services by design.

A PMP will among other things designate a responsible individual for the PMP, set out policies and programs for dealing with privacy impacts assessments and privacy breaches, and ensuring privacy training for employees.

I would emphasize that PMPs should be reasonable and scaled commensurate with the volume and sensitivity of the personal information the public body manages. In other words, a large public body that holds a vast amount of sensitive personal information will have a PMP that looks quite different from a small public body with minimal personal information.

Further specifics about what a privacy management program entails, can be found in my supplemental submission. It should go almost without saying that responsible management of personal information, central to a Privacy Management Program, is critical to build and maintain the trust of British Columbia citizens.

I fully expect my office will be asked to consult with a great many of the province's 2,900 public bodies on their specific PMPs.

Whether asked by the Superintendent of School District 71 in Courtney Comox, the CAO for the City of Kimberley, or the CEO of the Interior Health Authority, my policy team will be there to answer their questions, reviewing their documentation, and providing resources that facilitate their implementation of an effective privacy management program.

In summarizing these two new legislative requirements I am sure you won't be surprised to hear that I was very pleased to see they introduced together; the requirement to develop a privacy management program supports public bodies in protecting personal information before there is a problem, and the requirement to report breaches means that where problems arise my staff can support public bodies in getting things back-on-track, if that is what is needed.

*****

Now that I have given you a brief overview of the new requirements, and the anticipated impact on our office, I would like to address how we plan to ensure our office can implement the amendments.

We have established an integrated approach, that will permit breach notifications and PMP consultations to be processed efficiently, while education and enforcement work is carried out.

All of this is consistent with my broad mandate as Commissioner to ensure FIPPA's purposes are achieved through monitoring the Act's administration, informing the public about it, and conducting investigations, audits and complaint resolution that leads to legal compliance.

And we have already some take steps to revise our processes in anticipation of the increased demands I have

described for you tonight and done so in the following ways.

We have updated our case tracker system to get metrics for public reporting related to breaches and PMPS. These metrics will also help us tailor our education strategies, for example if we find there is a higher prevalence of certain types breaches among public bodies.

We have also established monitoring systems for processing voluntary breach notification files and mandatory breach notification files, and developed an early resolution process for breaches to determine whether they meet the real risk of significant harm threshold.

Ultimately, however, we will require additional resources to carry out the important responsibilities you as legislators have placed upon us. We have exhausted any flexibility to absorb the extra cost in our current budget that the amendments demand. Therefore, to ensure we are able to fulfil these requirements under Bill 22, I have put together a conservative request of 7.5 FTEs.

They include:

- 2 FTEs that will support intake, early resolution of breach notification, and basic requests for information about the new requirements on public bodies;
- 3 FTEs that will support processing the increase in mandatory breach notifications and any increase in investigations or audits related to public bodies not performing their breach notification or PMP responsibilities;
- 2 FTEs that will support consultations on PMPs, including privacy breach response policies, and complex requests for information. This is necessary to support public bodies to comply with the legislation and offer guidance in how to do so; and
- 0.5 FTE that will support education work through the OIPC website, presentations, and publication of investigation and audit reports.

We know that we will receive significant increases in requests for information, breach notifications, and requests for consultation on PMPS from public bodies. Therefore, we have factored in to our approach the need for our office to educate and consult with public bodies about privacy breaches and PMPs.

I am therefore asking the Committee for a supplementary budget request to support the OIPC in implementing Bill 22, of an additional $890,000 for operating costs, and an additional $16,000 for capital costs. These resources are required as a result of legislation that was passed and without them I will not be able to meet my responsibilities under the Act.

This will result in a total operating budget for fiscal years 2023/24 to 2025/26 of $10,162,000, $9,891,000 and $9,622,000 respectively. The resulting capital budget requested for the same three years is $277,000, $52,000, and $82,000 respectively.

Those of you who have considered my office's submissions over the years know we have been very careful in our requests – making sure we explore all efficiencies and alternatives prior to seeking any budget increases. This is what we have done here and I want to thank my team not only for their careful and considered work in helping put together this submission but the dedication they bring to the task of serving the people of BC.

With that Chair, I thank you and the Committee for your attention this evening. My team and I would now be pleased to answer any questions you may have.