Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

SPEECH TO THE

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

NOVEMBER 18, 2015

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER FOR BC

Honourable Chair, Vice-Chair, members of the Committee:

I am pleased to be here again.

Joining me is Deputy Commissioner Michael McEvoy.

You will have received a detailed written submission from my Office.

In it we make 20 recommendations for legislative change, including a duty to document, oversight of the destruction of records, mandatory breach notification and reporting, and stronger privacy management requirements that raise the bar for personal information protection in BC.

I would like to spend the next 25 minutes talking about these key recommendations, as well as answer the questions put to me by the Committee.

My slide deck is quite simple but will help guide you through my presentation.

Having reviewed the written submissions and presentations made to you over the past few weeks, I am heartened by the level of public engagement with the Committee's work.

It is clear to me that British Columbians take a real interest in their information rights.

I'd like to start by talking about those information rights, and in particular the duty to document.

Duty to Document

As Committee members will know, on Oct. 22, 2015 I released an investigation report called Access Denied. In it, I examined FOI responses within the BC government and made a number of recommendations for change.

Two of my recommendations have been referred to this Committee for study.

The first is a duty to document – which is a positive duty for public servants to create full and accurate records.

The second area of study is oversight of records destruction with penalties for non-compliance.

I thought it would be helpful to talk about why I think these legislative changes are needed… and what they would look like in practice.

The Case for Duty to Document

One of the main messages of my recent investigation report…and in previous reports by my office … is that access to information rights can only exist when public bodies **create** and **keep** records of the key actions they take and decisions they make.

I believe the duty to document is a critical element of good records management …which in turn supports good government. This is especially the case in a world dominated by digital communication channels.

Some documentation is taking place now – but if one were to take a snapshot today … it would be **incomplete** picture of the 'what' and 'why' of government decision-making.

The government's new *Information Management Act* defines and sets out the mechanisms for retaining 'government information' but leaves unaddressed the need to **create** the information in the first place.

Citizens may wonder how is it that **any** government can operate without creating information about its major actions and decisions?

How would an auditor come to understand the underlying basis or rationale for financial transactions, if there is no written documentation?

How would a lawyer, defending or initiating legal action on behalf of government, find relevant evidence?

And in a democracy… how does the public hold its government accountable… if citizens have no way of knowing how decisions are reached?

Yet, increasingly, access to information requests are met with replies of "no responsive records," a phenomenon reflective of oral government where **some** public officials do not write anything down.

A recent review into firings in the Ministry of Health was hampered by what the lawyer conducting the review called a "dearth of documents," meaning that the records that would normally be available in a situation where discipline was being contemplated simply did not appear to exist.

A duty to document would ensure that there **is** a lasting record.

Because the reality is people's memories aren't perfect. Civil servants retire or move on to new opportunities The bits and bites of information that isn't being documented can be essential to understanding, and following through on, the important decisions being made.

Duty to Document: Addressing the Critics

After the release of my most recent report, there has been considerable public discussion about the duty to document.

And there is some spirited debate about whether such a duty would be helpful or harmful.

Those who oppose the duty to document typically cite two concerns.

The first is that it will be cumbersome… forcing government officials to document every idea and discussion, regardless of its import.

But this is not what my definition of a duty to document entails.

A Duty to Document does not necessarily require the production of more records.

Rather, it requires the deliberate production and retention of records about specific activities.

In jurisdictions such as Queensland, Australia, where the duty to create records is legislated, public bodies determine what functions and activities they are responsible for, and what records they should create.

Records that are created are those that support a public body's purpose and operational needs. It's a statutory responsibility. This brings clarity to the process of determining when a record needs to be created or should otherwise exist.

The second concern about a duty to document is that the disclosure of government's inner workings will "chill" the decision-making processes that are so vital to good government.

Public servants, it has been argued, will be less willing to express frank views, including difficult "truths" that politicians may not want to hear, for fear they will be misunderstood if these views are publicly exposed.

However, our existing access-to-information law already takes account of this concern in the "advice and recommendation" exception under FIPPA.

Certain kinds of behind-the-scenes discussions are not subject to disclosure, thus allowing for frank discussions.

It does not follow that a duty to document will result in a duty to disclose.

What would a duty to document look like in practice?

Thinking specifically about the B.C. context, I believe the duty should encompass three key requirements:

FIRST, it should be expressly written into FIPPA. This would ensure the duty extends to all public bodies, not just core government as is the case under the IMA. This would also ensure that my office would have responsibility for independent oversight.

I don't think a duty to document in policy will suffice. I believe recent events have made it evident that there needs to be a clear and unequivocal duty in law.

SECOND, the duty to document should be flexible enough to allow public bodies of different sizes and lines of business to establish practical and meaningful categories of records to be created.

Consideration must be given to business needs, accountability requirements and community expectations.

For example, if a public body is making a decision to embark on a new program, staff would be required to document or record the decision and the basis for this decision to implement a new program.

A social services agency would be required to document a decision around granting a benefit to an individual.

A contract manager would need to document how a contractor's qualification and services were scored, in case they were challenged.

THIRD, there needs to be robust and independent oversight of a duty to document.

Oversight of destruction of records

Another issue explored in my investigation report and referred to this Committee for study is oversight of the destruction of records.

This is an issue of public concern in British Columbia and elsewhere in Canada.

We have an oversight gap in our laws.

FIPPA provides minimal oversight of destruction of records, and only in cases where a person obstructs a public body's response to an access to information request by destroying records

And the *Information Management Act* determines a schedule for the destruction of records by core government, but not for the broader public sector.

This means if documents are improperly disposed of outside of the FOI process – there is no mechanism for investigation or review.

In Alberta, the Information and Privacy Commissioner has the power to investigate compliance with rules in provincial statutes or of local public bodies on the destruction of records. The Alberta statute establishes the unauthorized destruction of records as an offence.

My recommendation brings the Alberta model to B.C. – with my office having the power to investigate the destruction of records under **any** B.C. statute **and** oversight over records destruction that is in contravention of rules or bylaws of local public bodies.

This oversight should also be supported by new, complementary offences and penalties under the Act. I will speak more about penalties and sanctions later in this presentation.

PERSONAL INFORMATION MANAGEMENT

I would like to turn now to some of the key recommendations I am making specific to the protection of privacy.

My recommendations, if adopted, will raise the bar and ensure that public bodies properly manage the personal information of British Columbians in an accountable way.

Breach notification

I'd like to start with my recommendation for mandatory breach reporting.

We trust public bodies with our most sensitive personal information. Health records, tax data, financial information, the list goes on.

And turning over much of this information is not optional – when we need health care, when we enroll our children in school, when we need the services of government… we have no choice but to hand over our sensitive personal information.

It seems as though every week, the public learns about a new data breach involving lost or stolen laptops, mobile devices, misdirected emails containing sensitive data, or employee 'snooping' in electronic records.

Privacy breaches carry a human cost. They put individuals at risk for identity theft and serious reputational harms not to mention loss of confidence and trust in government.

Breach reporting in BC is currently voluntary. My office receives reports of what we believe are only 1% of all breaches that occur within government bodies.

A voluntary regime means there is no clear threshold for reporting to my office, no consistency in when breaches are reported to affected individuals, and is therefore incomplete.

Mandatory breach notification would give **citizens** an opportunity to be made AWARE of those significant breaches, and take steps to mitigate them.

There should also be a legal requirement to report significant privacy breaches to **my Office**, so that our staff can assist public bodies to address the breach, its root cause, and prevent future occurrences.

B.C. would **not** be charting new waters with such a provision.

Newfoundland and Labrador and the Territory of Nunavut have such provisions in place.

Seven of Canada's provinces have mandatory breach reporting requirements in their health information laws.

And the federal government addresses breach reporting through policy.

In November of last year, I made a presentation to the Special Committee to review PIPA, FIPPA's private sector counterpart. As part of those consultations, I outlined why mandatory breach reporting would be an important addition to the private sector legislation. The committee agreed, and recommended in their final report that PIPA be amended to require that organizations notify both the Commissioner and affected individuals in the event of a privacy breach.

There should not be a lower standard for the protection of privacy in the public sector.

Privacy Management Programs

Privacy breach reporting is only one part of an overall privacy management program.

Just as public bodies must have sound financial management practices and frameworks, they must also take a comprehensive approach to privacy.

Canada's Privacy Commissioners have issued detailed, scalable and practical guidance that provides private and public sector organizations with a roadmap to implementing privacy management programs.

This Committee has an opportunity to take this work to its next logical step –an express legal requirement spelling out what public bodies need to do in order to effectively protect the privacy of individuals.

The Special Committee reviewing PIPA made this recommendation for the private sector. While there are some differences, in my view the obligations should be harmonized between these two laws to provide for the same privacy management requirements, including:

- Appointing an individual responsible for privacy
- Staff training
- Privacy policies
- Privacy breach response plans

Privacy management programs do not prevent every breach, but they go a long way to giving public bodies the proactive tools to mitigate privacy incidents and build trust with citizens.

We have begun to see privacy management implemented on a policy basis. For example, government has set out its own program. But the broader public sector – education bodies, municipalities, health authorities and crowns -- should also be implementing controls to effectively protect personal information.

***

Of course, all of the recommendations that I've talked about here and in my written submission require robust and **independent** oversight in order to be effective.

Before I move to our Q and A, I received two written questions from the Committee that I would like to respond to.

The first concerns health information and how it should be dealt with in this review.

Unlike most other provinces, BC does not have sector specific stand-alone health information legislation.

Depending on the provider of the health service, personal health information may be subject to FIPPA, the Personal Information Protection Act or the eHealth Act.

I believe British Columbians would be better served with a single set of rules that facilitate the flow of information between public and private health providers, ensure robust protection for patient information and establish a framework for vital public interest research.

It is not expected that B.C. will adopt a stand-alone law for personal health information anytime soon.

While this Committee is tasked with reviewing FIPPA, there are a number of recommendations that I am making that are particularly important for strengthening the protection of personal health information.

I believe the **breach notification** requirements I proposed would be of great importance in the health sector.

Whether it involves cancer treatment records, records of a person's hospitalization, mental health treatment, or the results of an HIV test, British Columbians share, by necessity, far more sensitive personal information with the health care system than any other sector.

Much of this information is stored in electronic form in large databases, which means the risks – and potential harms – of privacy breaches are greater than they were in the days of paper-based records.

Similarly I believe my recommendations around **data linking** are important in the health sector.

Currently there is a carve-out for data-linking rules for the health sector. I believe the rules should be applied to personal health information, which would make them subject to transparency and review.

My recommendations for **new offences and higher penalties** will match those in other Canadian jurisdictions.

There have been numerous reports of employee “snooping” in electronic health records in B.C. and Canada in the past year.

While it is not a problem exclusive to health information it has proven to be a particular problem in that sector.

A framework for sanctions

Finally, I would like to answer a question I received from the Committee about a framework for sanctions.

FIPPA currently authorizes penalties for two types of offences. General offences carry penalties for individuals up to $5,000 while privacy protection offences for individuals carry penalties of up to $2,000.

These penalties are among the lowest in the country.

Other provinces have penalties ranging from $10,000 to up to $50,000 per offence. Ontario has passed a bill that will increase penalties to up to $100,000 for individuals.

BC needs to come into line with these other jurisdictions and deter would-be offenders. I am recommending that penalties for general and privacy offences committed by individuals under FIPPA be raised to up to $50,000.

I also recommend two new offences: the unauthorized and willful destruction of records, and for unauthorized access and use of personal information (in other words, a “snooping” offence).

***

A quick post-script: While this is not in my written submission – I believe the Legislature should review FIPPA more frequently than every six years.
Given the fast pace of technological change, and the myriad of access and privacy issues that continue to wash ashore in BC, I believe a review every 3 or 4 years would allow Legislators to ensure information rights are protected on an ongoing basis.

This would not require a legislative amendment – the law as it is currently written states that a review should take place “at least once every six years.”
I leave that for the Committee’s consideration.
Happy to answer any questions you have.