CHECK AGAINST DELIVERY

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

SPEECH TO THE

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

JULY 21, 2015

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER FOR BC

Good morning Mr. Chair, Mr. Deputy Chair, Members of the Committee.

With me today are Deputy Commissioner Michael McEvoy and Pat Egan, Acting Assistant Commissioner.

It is a pleasure to be here to provide you with a broad perspective as you begin the important task of reviewing the province's *Freedom of Information and Protection of Privacy Act*.

My purpose here today is not to set out a specific agenda, but to give you my perspective, to put the current law in context and talk about the impact of this legislation on the citizens of this province.

A legislative review is a marathon and not a sprint. I will provide you a more detailed submission later in the fall – and am open to any questions you have both now and as this important process unfolds.

INTRODUCTION

Let me start from the beginning.

Although the federal government has had Access to Information legislation since 1983[1], British Columbians did not have a legal right of access to government records, or the records of other public bodies, prior to the introduction of FIPPA.

Before the province's *Freedom of Information and Protection of Privacy Act* (FIPPA) came into force[2] in 1993 citizens did not have a legal right of access to government records, though it should be said there were various pieces of legislation protecting citizen's privacy.

So if a citizen wanted information on – say – whether her child's day care provider was licensed or what its safety record was, she had to locate the administrator of that licensing program, write them a letter, and whether she got the information depended upon the (often unwritten) policies of that agency. And if she didn't get what she was looking for, there was little or no mechanism for recourse.

In other words access was an arbitrary matter. And if the information was forthcoming there were no timelines for delivery of the information and no independent review or right of appeal that allowed a citizen to inquire as to why the information requested was not forthcoming.
The passage of FIPPA thus marked an important milestone.

Citizens' privacy rights were 'codified' and their access to information rights were defined; exceptions to those access rights were identified and independent oversight – a Commissioner – was established.

And while this piece of legislation legally protects access and privacy rights… I want to stress that it was designed to be, and should be, a tool of last resort.

The law guarantees a right of access; it does not require that a person file an FOI request any time they seek information.

Today, there are access to information laws in over 100 countries around the world. [3] Similarly there are over 100 jurisdictions that have privacy or data protection laws.[4]

B.C.'s law combines the two into a single statute – public bodies have the critical task of making sure personal information collected from citizens is protected while also ensuring government is both open and accountable with independent oversight of both by my office.

[1] http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/menu-eng.html
[2] Legislation was passed by the Legislature in June 1992, and came into force in October, 1993.
[3] http://www.rti-rating.org/country-data
[4] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416

When FIPPA was first introduced in British Columbia, it was praised as being the best legislation of its kind in Canada, perhaps even in North America. State of the art, they said.

Even today, B.C. is still recognized as a leader in access and privacy legislation.

The Centre for Law and Democracy, which publishes an access to information report card for Canada each year, has consistently given BC the top score of all provinces.

This year, we placed second – outscored by Newfoundland and Labradors' newly overhauled access to information and privacy regime.

(By the way, I recommend that the Committee review the Newfoundland and Labrador report, issued in March 2015--good cabin reading for August!)

Within Canada, B.C. is consistently ahead of the pack, but on a global scale we are not.

BC's laws rank 32nd of 102 countries[5] – tied with Georgia and Uganda. We fall behind the UK, Brazil, Mexico, India, and many others.

This being the fourth review of FIPPA it is important to consider EXTERNAL trends affecting the operation of legislation as much as the INTERNAL dynamics of information rights in British Columbia.

Your work is critical to continuing the **currency** and relevance of the legislation.

MY PERSPECTIVE

As an Officer of the Legislature whose role it is to "oversee" the legislation, I think I am well situated to assess both the access element and the privacy element – what works and what might need some improvement.

"Oversight" means I am responsible for ensuring public bodies comply with access to information and privacy obligations. I also have the authority to adjudicate access to information and privacy disputes.

On both the access to information side and the privacy side, key factors which have changed since the last review are:

1. The rapid acceleration in the use of technology and the new challenges this presents both to privacy and access to information, AND
2. Global legislative trends dealing with issues such as 'accountability' and effective oversight.

[5] We slotted BC's results in with the other countries in the Centre for Law and Democracy "Global Right to Information Rating" -- http://www.rti-rating.org/

In my detailed submission in the fall, I will have some very specific suggestions for your consideration; however, today I want to provide a high level perspective of some of the areas I believe warrant your attention.

Technology presents new challenges and opportunities

The pace and intensity of technological advancement – our ability to create, store, use and share mass amounts of digital information and data - is at the heart of some of the biggest challenges facing privacy and access to information today.

We have moved from a paper-based system to an era where records are "born digital."

Every day, government employees are creating hundreds, if not thousands, of digital records, all of which must be stored and secured within government networks and then either disposed or archived consistent with the law.

On the **access** side there is our expectation that government information is made available proactively in ways that are easy to find, easy to search, easy to use and easy to reuse.

While core government responded to 8,377 specific FOI requests in 2014/15 (down from about 10,000 the year before), there is increasing interest in proactive disclosure.

Such disclosures would relieve some of the pressure on the system while promoting trust on the part of the public.

I note that the number of access requests to government is on the decline – there were about 15% fewer requests in 2014/15 than there were in 2013/14.

That number could decline even further if government moved ahead with proactively disclosing (for example) calendar requests, which accounted for 12% of all FOI requests made to government in 2014/15.

On the **privacy** side, there has been an explosion in the volume of information **about** us.

Let's not forget that citizens rarely have a choice whether or not to hand over their personal information to public bodies in exchange for services.

Our capacity to collect, store, and use personal information and data is advancing at a rapid rate. The personal data citizens are required to provide public agencies increasingly have **value.**

Public bodies are under growing pressure to use data analytics to "mine" personal data sets for the benefit of public-policy making and for compliance and enforcement purposes.

There is a certain amount of public unease in relation to the use and protection of personal information in our digital society.

There is a concern that the right to privacy and protection of personal information will be swept away by these data flows… and that the many ways our personal information is being managed and used is becoming increasingly incomprehensible.

While we commonly think of the openness principle as being focused on facilitating disclosure of information, it is also reflected in the rules that govern sound management of personal information.

The public can only be confident in how their personal information is being handled when they KNOW that public bodies are acting as responsible stewards of their personal information.

This is in many ways demonstrated by the information these agencies make available about how they are managing personal data. So transparency is a very important element.

In light of growing concern about new and emerging technologies and their impact on information and privacy rights, transparency and openness are essential to build public confidence in the information handling practices of public agencies – and trust is essential as our society continues to deepen the way we use digital information and reflect ourselves in that use.

Technology and the health sector

One sector that combines large amounts of personal information with challenging technology issues is healthcare.

There is great public interest in the potential of new technologies to change lives: think genomics, health wearables and health data analytics.

But our personal health information is the most sensitive information we provide to public bodies.

I have always believed, and have made many speeches expounding the view, that we can have robust privacy protection as well as health research using this data – but we have to proceed carefully.

What complicates the health sector is the patchwork of laws and legislative carve-outs that knit together the rules for personal health information protection.

Unlike most other Canadian jurisdictions, British Columbia does not have stand-alone health information legislation.

Government has announced its intended consultation on the future of personal information legislation specific to the health care sector.

I have called for stand-alone health information rules in British Columbia, and I hope that the consultations arrive at that same conclusion.

Until we know the outcome of that process, this Committee will have to consider the particular impact, and concerns, of the health care sector as you deliberate on the future of FIPPA.

As you listen to and analyse the public submissions, I ask that you actively consider whether health information (increasingly part of an integrated system that operates across the public and private sectors) needs specific rules within our legislation.

Global Trends

On the topic of global trends, it will be of interest for the Committee to know that there have been significant developments in law reform in various jurisdictions over the past several years.

In Canada, we have seen amendments to the federal private sector law and as mentioned earlier, a far-reaching overhaul of legislation in Newfoundland and Labrador.

In the European Union there has been much work done to update the data protection framework – work that is on the cusp of being finalized.

This EU Regulation is leading edge, and will apply to the 28 members of the European Union – replacing domestic laws. Six years in the making, I consider that the EU Regulation will set a very high bar with respect to privacy management, mandatory breach notification, sanctions, and oversight.

When we look at these Canadian and global law reform initiatives, some important developments emerge.

Accountability

One of those big trends is explicit accountability requirements for public bodies written into law.

The word accountability likely means something very specific to you as legislators, or to your constituents – but let me describe for you what it means in terms of privacy and access to information.

Applied to **personal privacy**, accountability means that public bodies have a legal duty to take seriously their responsibility to protect the personal information that's entrusted to them by citizens and employees.

I believe there is a demonstrated need for specific accountability measures in our privacy law, to make sure the rules that public bodies follow are comprehensive and protect personal information in their care.

While a high level principal of accountability is in B.C.'s law, the specific accountability framework public bodies must take to adopt privacy protections is not.

Some elements of an accountability framework would include: mandatory privacy training for staff that handle sensitive personal information; privacy policies that account for how personal information is collected, used and shared; transparency reporting for disclosures to law enforcement; audit controls to monitor access; and have data breach response plans in place.

Another significant trend is mandatory breach notification, which ensures that when a data breach happens, affected individuals are notified promptly – so that people can take steps to protect themselves – and that my office is advised, to ensure we can exercise our oversight role of ensuring the breaches are managed appropriately and that prevention measures are taken. Currently we receive notices of less than 1% of government and health authority data breaches.

Breach notification is required by a directive in the federal public sector and is legislatively mandated in Newfoundland and Nunavut. Six jurisdictions across Canada require breach notification in their health information statutes.

The proposed EU Regulation is moving toward mandatory breach notification for both the private and public sectors, with significant sanctions for non-compliance.

There is a growing expectation that organizations and governments will be accountable to their customers and citizens, and to the public, when a breach happens.

You may be aware that the Special Committee that reviewed PIPA recently recommended mandatory breach notification and reporting for the private sector in BC.

I believe it is time to consider a similar recommendation for mandatory breach reporting for the public sector.

Public bodies need to move from being reactive to events like breaches, to being proactive. A comprehensive, systems approach to privacy that is written into law will help us achieve that.

I know that government has done a lot of work in developing a comprehensive approach to privacy management in ministries.

Many jurisdictions around the world are moving to implement explicit accountability requirements into their legislation and policies – the Special Committee to Review B.C.'s PIPA also recommended such language be included in B.C.'s legal framework as it applies to the private sector.

This Committee should consider similar amendments to FIPPA to make clear what a public body's obligations are to protect personal information in a proactive way, but I will have more to say on this in my detailed submission.

Applied to **access to information**, accountability means a number of things.

It means public agencies making information available to citizens in open and re-usable data formats. It means information being made available proactively, rather than in response to an access request.

And it means public bodies having a legal responsibility for the full life cycle of a record – from creation to final disposition.

Accountability in access to information practices drives discussions about the need for a duty to document key actions and decisions of government, proper records management and archiving regimes and ensuring that information is not deleted or destroyed in an unauthorized manner.

When records are properly created, managed, preserved and disposed of then citizens, businesses, non-profits and others get optimal use out of our laws to better understand government and participate more fully in our democracy and society. I believe this represents good government.

<u>Effective Oversight</u>

Another global trend with respect to both the access to information and privacy elements is that of increased authority for independent agencies that provide oversight for the legislation.

Effective oversight means things like having the legislative authority to ensure there are proper management systems in place for documents and personal information.

I think of information in the same way accountants think about financial assets – the key is proper management systems and processes to ensure records and information are handled appropriately.

Effective oversight means ensuring that the only records destroyed are authorized to be destroyed by legislation and policy. It means that the government and other

public agencies can account, through record keeping and documentation, for what has happened to records or personal information when called upon to do so.

These duties require independent oversight and, as in Alberta and Ontario, this oversight should be located in FIPPA. It may also mean providing administrative penalties and sanctions for deliberate destruction of records.

I will have more detailed proposals reflecting the global trends in effective oversight in my presentation to you in the fall.

FROM CHALLENGES TO VALUES

These technology challenges and global trends tell us that the world of privacy and access to information is constantly evolving and that if BC wants to stay current, our legislation must evolve.

While there is merit in dealing with specific problems by addressing specific clauses of the legislation, I suggest this be done within the broader context of defined values.

FIPPA has some important values embedded in it and I think this lays a solid foundation for future amendments.

The values that I think should continue to underpin any recommended changes the Committee may make are: Trust, Transparency and Accountability.

Where there is no public TRUST, there is no public confidence. Where there is no public confidence, public agencies have a really hard time implementing new programs, especially those that involve new technology.

This is why when considering any potential changes to the law, I encourage the Committee to assess whether the public would consider what you are doing as promoting the building of TRUST in public bodies … or eroding it.

The second value is transparency.

Transparency is critically important to the integrity of the operations of a public body, and is essential to getting buy-in from the public as government agencies increasingly shift their operations to the digital realm… it is also the foundation of proactive disclosure regimes and lawful responses to access to information requests.

When considering any changes to the law, I urge the Committee to consider how greater transparency can be achieved – including such ideas as “open by default.”

Finally, there is accountability.

Public bodies need to be able to explain how they use personal information and how they process requests for records and be willing to be held accountable for these explanations and processes.

As demands for accountability grow, the Committee should consider how their proposals enhance accountability for personal information in the possession of public bodies and for their processing of information requests.

CONCLUSION

Your committee will, I believe, be receiving a large number of submissions.

Many will deal with specific issues, such as the fee structure applied to access requests, or steps to make it easier to store government data outside Canada or in the 'cloud.'

Many will be broader in scope, such as suggestions to improve access to public agencies' information, to encourage more proactive disclosure and for a duty to document to mention a few.

My guidance for your consideration is – the principles that underlay access and privacy rights in FIPPA remain fit for purpose.

I think it is important to maintain the fundamental principles and not move away from them -- while updating our law to deal with developments created by technology challenges and by new access and privacy legislative developments in other jurisdictions.

The Act is not without its critics, but in providing a largely free and universal right of access to information, subject to legitimate exceptions, and protection for citizen privacy -- the current law is a solid foundation on which we can build a yet stronger legislative framework.

I am very pleased that this committee has been established and look forward to providing my detailed submission later this year.

Finally, I would like to invite all of you to attend the conference my office is hosting November 12-13 in Vancouver. It's called *Privacy and Access 20/20: The Future of Privacy*. Registration is already open. We've got a great agenda coming together and I look forward to welcoming you all there.

Thank you for your attention this morning. I look forward to questions.