Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

KEYNOTE SPEECH TO THE

BC-CANADIAN BAR ASSOCIATION ACCESS & PRIVACY SUB-SECTION

MAY 13, 2015 – VANCOUVER, B.C.

BY

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER FOR B.C.

I apologize for my delayed arrival today. We received a last-minute request to appear before the Finance and Government Services Committee of the Legislature. They wanted to know what our office has been up to over the past six months. This is the first time the Committee has met with us other than the annual budget submission meeting and as an officer of the legislature I appreciated the opportunity to be accountable. That was bright and early at 9:00 a.m. this morning at the BC Legislature!

I want to thank you again for inviting me. Thanks especially to Sara Levine and Ryan Berger. This is the sixth time I have been asked to present my thoughts to the CBA Access and Privacy Subsection and I welcome the opportunity because of the role you play in interpreting access and privacy legislation and providing advice to your clients and organizations on these important matters.

Let me start my speech by trying to predict the future by telling you what I think is coming down the privacy pipe. Then I'll give you a quick update on some of the major files on my desk recently. Let's start with some crystal-ball-gazing into the future.

PREDICTING THE FUTURE

I suppose it's not hard for anyone in this room to predict that privacy will keep making headlines. In a world where massive data breaches happen every day, surveillance is ubiquitous, and advances in technology happen in the blink of an eye, how could privacy not be continuing front-page news? What I am seeing on a day-to-day basis, however, and what I think is particularly interesting, is the significant increase in requests for information from the public—engagement of the public.

Early data from our forthcoming annual report shows us that emails and phone calls and messages from the public have spiked—we received 5,200 requests for information in the 2014/15 fiscal year. These are not case files, appeals or complaints: these are questions about what the law says, or how the Commissioner's office can help. To put that number in perspective, in my first year as Commissioner we received 3,750[1] requests for information from the public. So last year's total represents a 40% increase over five years.

This demand for information is driven by new and emerging technology, the explosion of privacy breach stories in the news, and other developments that make risks to privacy and personal information very real to British Columbians. At the same time we've seen ongoing increases in what I call our bread-and-butter files.

[1] I am using 2010-11 numbers from the Annual Report to illustrate the data in your first full year as Commissioner.

Privacy breaches: in my first year as Commissioner we had 65 breaches reported to our office. This past year: 132. An increase of more than 100%. Privacy impact assessments: from 7 PIAs in 2010 to 33 this past fiscal year. That's a 371% increase in five years. Policy or issue consultation: 62 five years ago, 170 today. All of this to say that citizens, consumers and employees are thinking more about their privacy in all contexts, and public bodies and organizations are engaging our office more frequently.

While this work keeps me and my excellent staff extremely busy, it shows us that what we do does matter to citizens. And it shows us that individuals care very deeply about their privacy and access to information. And they look to members of this community—to privacy counsel, privacy practitioners, and to regulators—to ensure our laws are strong and robust enough to protect their privacy in the digital age.

National Security and Surveillance

I would also predict that we will continue to hear about the growth of national security and intelligence-gathering activities in Canada. Of course Bill C-51 has been the focal point of these debates. I am very disappointed to see that C-51 has passed third reading in the House of Commons since I and the other privacy commissioners think the balance between security and personal privacy has been dramatically altered on the side of security. I was also disappointed in the lack of engagement with privacy regulators in Parliament's review of C-51. The fact that federal Privacy Commissioner Daniel Therrien was not even invited to appear before the Standing Committee on Public Safety—the committee studying the Bill—is a very difficult decision to accept. As an agent of Parliament, the lack of an invitation to appear before a Parliamentary Committee to speak to the privacy aspects of the Bill is, in my view, very unsettling in a democracy such as ours.

Despite the fact that C-51 has passed through the House of Commons and is now before the Senate, I think public concern about these issues will continue to boil over in the media, in Parliament. This is because Bill C-51 mandates over-broad, unregulated and what I believe to be intrusive sharing of personal information. It grants 17 federal departments and agencies broad new authority to share personal information… including information of Canadians not suspected of terrorist activities, for the purpose of identifying new threats. The business case for why these new powers are needed has not been made.

In October 2014, several months before the Bill was introduced, Information and Privacy Commissioners federally and from every province and territory across Canada signed a joint statement calling for:

- an evidence-based approach to any proposed increase in powers;
- an open dialogue on whether additional measures are required; and
- that any new powers come with enhanced oversight for intelligence and law enforcement agencies.

After C-51 was tabled, provincial and territorial Commissioners from across Canada renewed our objections to the Bill and in a joint public letter on March 4, 2015, urged the federal government to amend C-51 to remove the most offensive portions in terms of the impact on Canadians' privacy. I do not believe the deep public concern about this legislation is going away, particularly when the legislation begins to be applied

Privacy Breaches

Looking once again into my crystal ball, I see more and more privacy breaches by business and government agencies. Some have called 2014 the year of the data breach. And I expect that in 2015 we will see the scope and volume of privacy breaches continue to grow. What I think is noteworthy in terms of the future discussion, is that B.C.'s laws are poised to evolve to address the question of how and when individuals are notified when privacy breaches happen. I think the dialogue about breaches will move from a place of "oh @#$% another privacy breach" to "what can we do to mitigate the risk of breaches from happening in future?"

Mandatory Breach Reporting

Some of you will know that in 2014 the BC Legislature struck a special committee to review PIPA, B.C.'s private sector privacy law. One of my major recommendations to the committee was for mandatory breach notification—this express legal amendment would require individuals to be notified of major breaches, and that those same breaches be reported to my office. The threshold we recommended was in cases where there is high probability of significant harm to the individual.

The case for mandatory breach notification is that it gives individuals an opportunity to protect themselves from privacy harms, but it also gives my office an opportunity to assist organizations and sectors address the root causes of breaches and engage in learning about trends and future prevention. I am pleased that the Committee has endorsed this recommendation, along with the other recommendations my office made in the PIPA Review process. I further predict this conversation will make its way to our public sector legislation in 2015-16. Has the time come for mandatory breach reporting for government and public bodies?

I am currently studying that very question by way of our new audit and compliance program—which I will touch on a little bit later.

Law Reform

My final prediction for the future is that of law reform. There are a number of different pots on the stove right now in this regard. As I just mentioned, we saw the PIPA Review Committee wrap up their review of our private sector legislation in February 2015. Their final report, which contained 15 recommendations, is currently with government for a response.

And B.C.'s FIPPA is slated for review in 2016. It may begin earlier than this depending on whether there is a Fall legislative session. I expect many of you in this room have ideas about how our public sector law could be updated and modernized. We also know that the Ministry of Health is currently consulting with stakeholders about a comprehensive health information law. I am encouraged by this development and we expect to hear more about this throughout 2015…

We also have the *Information Management Act*—which is before the B.C. Legislature updating the antiquated 1936 *Document Disposal Act.* As far as privacy and information management goes, that's a lot of legal reform underway, or about to begin. Some of these Bills, like the *Information Management Act*, is the first time in a generation that it's been looked at. It's a fascinating time, but also a critical juncture to be thinking about how our laws work. Each of you in this room will be looked to to play a role in all of this. I will reach out to you, your clients will look to you because of your window on these issues—you play a pivotal role in law reform!!

Summary

These are just a handful of the privacy-related topics that I think we will be hearing a lot about in the coming year. Of course, I restricted my comments to what is going on in Canada. I could've gone on for a lot longer if I were to talk about what is coming down the pipeline in the United States, Europe or in Asia. Lawmakers, academics, regulators and practitioners around the world are grappling with new and challenging privacy and access to information problems.

RECENT CASES

I would now like to review some of the major files that have been on my desk and on my mind lately.

Saanich Investigation

My office's latest investigation report concerns the District of Saanich's use of employee monitoring software on workstations of a number of employees and councillors. This information came to light when Mayor Richard Atwell held a press conference, alleging he was being spied on by the District and that the software had been installed to secretly monitor his activity.

In the media commentary that followed, Saanich Council made public comments that stated employees have no reasonable right to privacy in the workplace. As Commissioner, I could not let those statements stand. And I could not ignore the growing number of questions about the use of employee monitoring software by the District. So I initiated an investigation on my own motion to examine whether the use of this software complied with FIPPA.

It was important to me that our investigation was completed quickly, and efficiently in order to provide definitive answers to the questions that were floating out there in the public mind about Saanich's alleged spying software. We launched the investigation January 20, and we issued our public report on March 31, 2015.

Our investigation found that Saanich picked an off-the-shelf solution as a quick fix. District staff explained to my investigators that Saanich had an incoming tech-savvy Mayor and senior staff wanted to move quickly to address some of the District's known IT vulnerabilities. They selected a program called Spector 360, and enabled invasive tools that captured an employee's every keystroke and email, and pictures of screen activity every 30 seconds. These tools vacuumed up not only work data, but also the private information of employees including online banking transactions, confidential correspondence, and private passwords or images.

Ironically, Spector 360 created a security risk for the District because it actually amassed a data haystack of interest to parties with malicious intentions, and the District failed to implement any access logs or audit controls. My main recommendation in this report is that the District of Saanich disable these key functions of their employee monitoring program and to delete all the data collected by the software.

I also recommended that Saanich appoint a chief privacy officer to lead the implementation of a comprehensive privacy management program for the District.

District and Council has agreed to implement all of my recommendations and agreed to delete all the data collected by Spector 360 when it was operational.

Breach Examination // Audit and Compliance Program

I'd like to change gears here and talk about a special report I released in January of this year examining the BC Government's privacy breach management. This is the first report in our new audit and compliance program. Details of this program, including its charter are on our website. I selected core government for this audit because ministries are entrusted with a large amount of sensitive personal information.

And given government's unique role as a provider of public services to British Columbians, we expected they would be 'best of breed' in how they manage privacy breaches. We knew going into this audit that government already had a centralized model that manages privacy breaches and information management across all ministries, under the auspices of the CIO.

And we learned a lot of interesting things about the number and type of privacy breaches government responds to. For example, from 2010 to 2013 there were 3,800 suspected privacy breaches and 2,700 actual privacy breaches. About 70% of

breaches are “administrative errors” and a great number involve a single record gone missing—such as an email sent to the wrong person or a double-stuffed envelope. By far the smallest number (1%) of privacy breaches were the result of cyberattacks or phishing.

There are many merits to government’s centralized model. Suspected breaches are being reported quickly and investigated promptly. Notification to individuals occurs when needed, but, in my opinion, the current model doesn’t go far enough. There is currently no follow up by the CIO or analysis of breaches across ministries, and nothing in place to make sure privacy and security recommendations are implemented.

We recommended that government be more proactive about breach management – the key advantage to a central agency approach is to be able to scan the horizon, to see major issues as they arise, and address trends and vulnerabilities in a systematic way.

There were also findings regarding breach reporting to my Office. There were serious privacy breaches that I would have expected us to have been notified about but were not reported to our office. Reporting to the OIPC appears to have happened on a subjective basis rather than against a written or established policy or standard. One of the key recommendations coming out of this audit is that there should be a threshold against which government measures all its privacy breaches and if they meet the criteria that they are reported to my Office.

Our next steps will be to look at the breach management practices of other public bodies—including a municipality, a health authority and a university—with an eye to both suggesting improvements in the management of breaches, the notification practices to citizens, and disclosure to our office, and to whether an express breach notification provision is needed for the public sector.

Mount Polley

Finally, in the “coming soon” category, I wish to make a couple of brief comments about my office's report of the Mount Polley incident, which will be published very soon.

In 2014, we received a complaint and announced that we were investigating whether government was legally bound to disclose information about the Mount Polley mine to British Columbians under s. 25 of the *Freedom of Information and Protection of Privacy Act*.

Section 25 of FIPPA imposes an obligation on public bodies to provide citizens with timely information in two circumstances: where there is an imminent and significant risk of harm to the environment or safety of the public; or where information is, for any other reason, clearly in the public interest. A duty to warn and a duty to inform.

In December 2013, I released a comprehensive investigation report about a public body's duty to warn under s. 25 of FIPPA. Through that investigation it became clear that public bodies did not fully understand their obligations to inform the public in such cases. The report made three recommendations, including a legislative amendment that would mandate public bodies to disclose information in the public interest, even where the information is of a non-urgent nature. As my investigation into Mount Polley concludes, I find myself once again considering this issue of the threshold for public interest disclosures under s. 25 (1)(b) of FIPPA.

I anticipate our report into the Mount Polley incident will be released next month. I hope that you will all consider the analysis I have put forward on this critical provision of B.C.'s public sector law.

Conclusion

Thank you for your attention this afternoon. I look forward to any questions you may have.