CHECK AGAINST DELIVERY

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

"News and Views from BC's Information and Privacy Commissioner"

Elizabeth Denham, Information and Privacy Commissioner for B.C.

Presentation to the
Continuing Legal Education Society of BC
Vancouver, BC – May 1, 2013

Good afternoon everyone, and a friendly hello to those of you joining us via webcast!

Thank you to Monica Muller and Sara Levine for the invitation to speak today. Monica and Sara know how much I enjoy speaking to the access/privacy subsection of the CBA, but it's my first CLE event, so I'm very happy to be here.

It's fitting that you are all gathered here at CLE-BC for a privacy update during privacy awareness week!

For those of you not familiar with this initiative, it originated with the Asia Pacific Privacy Authorities – known as APPA – of which BC is an active member. The purpose of the week is for us to recognize the value of privacy, and the importance of protecting it. APPA created an infographic to mark this year's theme, which is the intersection of privacy and technology—and how technologies are creating new privacy risks. I think it's the right theme, especially given what's been happening here in BC and beyond!

New technology is doing more than changing how we access and store information. It is creating new dynamics, new opportunities, and new challenges for all of us—regulators, businesses, government, and citizens.

The growth of internet technologies, Wi-Fi, and mobile devices has increased our collective appetite for data. The amount of user generated content uploaded and shared online, everything from Instagram photos to YouTube videos, blogs, wikis, and social networking, is growing as a total share of online content. Most of us are shopping on-line, banking, gaming on-line, even dating on-line! We've come to expect more services, including government services, at our fingertips.

All of these functions require a certain amount of personal data to be shared, which raises important questions about data security and how our information is being protected. After all, new technologies collect information about us that was not previously quantifiable, and a lot of it is personal information.

We post to our timelines on Facebook, check in on Foursquare, upload photos to Flickr and Instagram, and connect on Twitter. We trust these programs with the images and stories of our lives, and each and every one of our stories can now be quantified, and monetized. This is not just an online phenomenon.

A photograph of your face can be used to create an algorithm as unique as your fingerprint. It's called facial recognition technology, and it's being used by organizations like ICBC to detect and deter fraud. Municipal and federal police forces are using automated licence plate recognition to capture licence plate data and compare it to an alert listing of drivers who are of interest to police. GPS-enabled smart phones are beaming back information about your location, in some cases, even when they are turned off! Now that's creepy. And in some parts of BC, smart meters have begun collecting details about our hourly energy usage and transmitting that data wirelessly back to BC Hydro on the smart grid.

The bottom line is that these technologies are by design able to quantify and collect new and more granular information about who we are and what we are doing. Technology allows public bodies and organizations to provide exponentially increasing levels of services to greater numbers of citizens, at remarkable speeds compared to paper-based systems.

But information systems also enable personal data of potentially millions of individuals to be disclosed very quickly to unauthorized recipients with potential harm to those affected. Privacy breaches are always making news – such as the University of Victoria's payroll information breach and also a data breach we're investigating right now that involves information technology at the Ministry of Health.

This past year, we were notified of more than 105 data breaches – many of them involving lost or stolen laptops, unencrypted USB keys, or unauthorized access to information within a company's system. That's more than a 25% increase over last year and 75% higher than it was two years ago.

There is an inherent tension between the public desire to leverage these new tools and public concerns about privacy and the protection of personal information in the wake of these technologies. This is the new frontier in privacy protection. What happens in the next five years will shape the future of privacy for generations to come.

I am particularly concerned about the use of these new technologies by the state. While there are concerns relating to privacy and technology in the private sector, particularly around social networking, people still have a degree of choice about where they want to play and how they share their personal information. It's one thing to choose to share our information through Facebook or through Twitter, but it's another thing to look at what government is actually doing with our personal information.

Governments are entrusted with citizens' data. How that data is used, linked and shared, can affect our life and our ability to get services…to get a job. We don't get to decide whether or not to provide our personal information in exchange for health care or other government services, like a driver's licence, photo ID or a passport. No institution has greater access to personal information of British Columbians than government.

The privacy challenges posed by the implementation of digital technology in the public sector is becoming a major component of the work of the OIPC. I would like to take this time with you today to review some of the strategies my office is undertaking to grapple with these important issues.

Proactive Review of New Technologies

Our first strategy is prioritizing proactive reviews of new and emerging technologies. One of our most critical roles is to ensure that government addresses and mitigates privacy risks before it implements new programs and new technologies. Some of the examples of the programs we've previewed in the last year are the BC services card, the integrated case management system and the Provincial Health Services Authority's picture-archiving system, all of which involve a great deal of information-sharing and integrated programs. Again, building privacy and security controls at the front end ultimately saves the government incurring costs from changes that are required after private data has been compromised.

Each year IT becomes more advanced and more complicated, and requires ever-increasing expertise to identify risks and mitigate them. We embrace those challenges, but it's becoming clear that our office requires technical expertise if we're going to continue to meet the scale and complexity of these challenges. We are simply outgunned without technical experts on staff. To assist us in addressing these challenges, we are fortunate to have received new funding for technical experts.

I'd like to take just a moment to talk a bit more in depth about our review of the BC Services Card, because it is one of our biggest files this year.

The BC Services Card is the first program of its kind in Canada. This program will collect, use, and disclose the personal information of virtually every British Columbian. And future phases could enable multiple government services to be accessed online. It is critical that the card be built with robust privacy protection by design.

My office has completed a review of Phase 1 of the BC Services Card, which is limited to the enrollment of individuals and issuance of the card, built around a provincial Identity Assurance Service. Our review included an examination of the legal authorities for sharing data, and a review of the technological systems and security measures in place to protect personal information. We found that the issuance of the BC Services Card, and the initial systems needed to support it, meet legal requirements. However, we made several recommendations to enhance the existing privacy and security provisions for Phase 1 of the Card.

But it is the next phase—which gets us closer to the world of online government services—that requires even more searching examination. Phase 2 will be a significantly larger step that brings with it considerable risks to personal privacy, in that there is the potential for data linkages to connect our discrete activities across multiple platforms. Given the program's profound reach and the amount and type of personal information involved, it is critical that citizens are included in the dialogue. My major recommendation going forward is that government conduct a fulsome public consultation with British Columbians before the BC Services Card program proceeds to Phase 2. Government has agreed.

My office will continue to watch vigilantly as the phases move forward. We will conduct quarterly reviews over the next year to verify that proposed security measures outlined in Phase 1 are being implemented, and to provide a thorough review of the proposed functionality of Phase 2. We know those who are designing the program are also well aware of the need to get it right.

This is just one example of the ongoing work my office is doing to ensure new technologies include robust privacy protection by design.

Systemic Investigations

Another area where we have been quite active: systemic investigations. These are Commissioner-initiated investigations where we get to take a deep dive into a particular issue, technology or service in order to explore its contours and assess the access or privacy implications for the public.

We use our regulatory powers to promote debate and dialogue about privacy by providing citizens with detailed information about how these things actually work. A critical role for offices like mine is to pull back the curtain to shine a light onto the far

corners of a program, technology or issue on behalf of the public… so that citizens can decide for themselves whether a particular technology or practice is OK or whether it's creepy.

Commissioners are uniquely placed to do this work. The law gives me the authority to conduct systemic investigations and proactive assessments. When we exercise that authority, we dive deeply. Our ability to conduct this type of investigation on our own motion goes hand in hand with our role as an enforcement agency. Without it, we could not properly protect British Columbians' personal privacy rights. And, as data processing becomes more pervasive, unobserved and complex, how would the average person even know what to complain about?

We achieve both of these aims – enforce the law, and provide the public with the information they need – by being as transparent as possible about our work, and by publishing the granular details of our investigations when it is in the public interest to do so.

We've published several investigation reports in recent months, including a review of the BC Government's use of criminal record checks, the Victoria Police Department's use of Automated Licence Plate Recognition technology, and a review of the BC Government's "no responsive records" replies to general access to information requests.

Some of our upcoming reports include:

- A review of BC's open government initiative
- An investigation of the use of the section 25 provisions (health and safety notifications) by public bodies
- A data breach at the Ministry of Health

All of these reports will be coming out in the coming weeks.

Accountability

The last thing I want to mention before welcoming your questions is an initiative of Canada's Privacy Commissioners to get organizations to adopt privacy as the default setting.

"Getting accountability right with a privacy management program" is a joint product of the Office of the federal Privacy Commissioner, the BC office and the Alberta office. We worked together on this project in order to provide clear, consistent guidance across jurisdictions that would address the core compliance issues we've collectively observed over the better part of a decade. The bottom line is this: Many organizations say that protecting privacy is important to their business, yet they fail to implement the necessary measures to create a culture of privacy.

Even after a decade under PIPEDA and almost a decade under PIPA, many do not have policies, practices, training or audit mechanisms in place to assess how – or how well – personal data is protected. "Getting Accountability Right" gives you a roadmap to becoming accountable, with sound data management practices underpinning the entire operation.

The paper takes a building block approach to implementing privacy management, beginning with an organizational commitment to a privacy-respectful culture. Next are the program controls, starting with a documented inventory of what personal information is held, where it is held, its level of sensitivity and the purposes for which it is being collected, used and disclosed. Third, ongoing assessment and continuous improvement is critical in light of changing threats and risks.

With this document comes a shift in expectations among Commissioners in terms of enforcement and audit activities. Instead of focusing exclusively on reactive investigations, for example in response to a complaint or a story in the news, we are developing guidance, issuing directives and launching systemic reviews on our own motion in order to be more proactive in addressing privacy and security issues.

We are encouraging comprehensive programs for data protection, ensuring companies and public bodies have the capacity to manage privacy and use new technologies responsibly. And with the accountability framework, we've put organizations on notice that we expect to see evidence of a privacy management framework in place as part of our enforcement work.

We've applied a privacy management lens to several recent investigation reports, including the privacy and security of wireless smart meters, a privacy breach at the University of Victoria, and an examination of facial recognition technology by the Insurance Corporation of British Columbia. What we have found is that shining a light on the practices of an organization in a particular sector creates incentives for others in that sector to get on board.

I am also extremely pleased to see organizations and public bodies adopt the guidance and framework proactively. For example, the BC Lottery Corporation is leading by example and has made an organizational commitment and built privacy into its management processes, including internal audits.

Following the investigation report into the University of Victoria, several universities—including of course the University of Victoria, and UBC—have begun implementing privacy management across their campuses.

We have also had interest from other data protection authorities. The Hong Kong Office of the Privacy Commissioner is using this document as a basis for their enforcement activities. So we have had some successes—but there is more to be done.

In BC we are adapting the guidance to fit the unique needs of the public sector. While we have seen some uptake with the accountability guidance among some public bodies, these organizations have unique challenges and we are creating tailored guidance to help them build a culture of privacy. Look for this guidance in the coming weeks.

Wrap-Up

In all of these areas—systemic reviews, proactive reviews, and through mechanisms like the accountability guidance— we are trying to stay ahead of the game and provide sound advice when it comes to the interaction between new technologies and personal privacy. There are a lot of questions out there about where this is all headed – and we are hoping to provide at least some of the answers.

For more information about these and other initiatives, I encourage you to visit our website, to follow us on Twitter and check out our guidance materials including the ones I've mentioned here today.

Before I turn the floor over to questions, I would like to take this opportunity to shamelessly plug our upcoming conference—Privacy and Access 20/20, Vancouver, BC, October 10-11, 2013. Agenda in coming weeks online so stay tuned.

I am open to any questions that you may have.