Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

SPEECH TO THE

BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION (FIPA) INFORMATION SUMMIT

SEPTEMBER 19, 2014

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER FOR BC

I'd like to start by thanking Richard Rosenberg, Vince Googolek and the FIPA board for the invitation to speak today. We have for many years, and continue to be, proud supporters of the information summit.

It's great to be here as we kick-off Right to Know Week! While access to records and FOI is part of our shared lexicon, it's important to shine a light on why access rights matter to the average person. Right to Know week, and the work you do putting on this conference, is a great way to make that happen. My Office too intends to contribute to the public conversation around the Right to Know week.

I can tell you, that next week, I will be issuing a Special Report on the BC's government timeliness in responding to access to information requests. It's been a while since our last report card and I thought it was very important to return to this issue because it underpins so much about the public's right to know. We've spent the last few months looking under the hood at ministry performance and we will have something significant to say about how government is doing on the timeliness front.

Now I am not going to issue a spoiler alert at this point but I can say but the short title of the report is *A Step Backwards*. The report also contains an important update on a concerning trend of no responsive records—that is to say, requests for records that come up empty, which you will recall my office examined last year. So please look for that report next week.

As I was preparing for this speech today, I was astonished to realize that it has been two years since the last FIPA Summit! I'm now in the home stretch of my six-year term, with just eighteen months to go. As they say…time flies while you're having fun! Also having fun here with me today are Michael McEvoy, Deputy Commissioner and Brad Weldon, our senior policy analyst and speaker on the whistle blower panel this afternoon.

It has been a crazy busy time for our office—everything from data breaches at retail giants like Home Depot—to tailings pond breach at the Mount Polley mine in northern BC. From the revelations about intelligence gathering in the US, Canada and beyond—to the 33% increase in individual complaints and requests coming through our front door. There has been no shortage of work hitting our desks. I'll admit it's been challenging keeping up with an increasing workload and the added complexity of files with limited resources.

Choosing what to do, when to do it and what tools to use in each case is the trickiest part of my job. With every file and every issue, we have to decide which hat to wear: advisor, counsellor, mediator, police officer or judge. And the reality is we simply can't chase every rabbit! This is especially true for our proactive work, where we investigate an issue on our own motion and dive deeply into a new program or technology.

Our dance card on that front is pretty full these days. From an audit of breach management practices of the BC Government, to an investigation about whether the Mount Polley breach should have been reported to the public, to a recent request from FIPA to look into the personal information collected by police departments about prospective employees and volunteers.

As you can imagine we have an endless array of candidates for systemic investigations—more than we can possibly undertake. For that reason, we have to be selective in order to be effective. Some of the big files we've tackled recently include: police information checks, the duty of public bodies to warn and inform under section 25 of FIPPA, the state of health information privacy, and the dire state of government archives.

Add to this the fact that new and emerging technologies continue to be an important part of our work, especially in the context of the public sector. We've put a sharp focus on evaluating new programs such as the BC Services Card, tokenization, and the integrated case management system. In short, we are energetically focusing our resources on the issues, programs and policies that have the greatest impact on the access and privacy rights of British Columbians.

We must also be sure that our work continues to be relevant and that we reach out to share our message—in particular with the general public and the media who impart much of the message to the public. I deliberately use the word *we* in describing this challenge. You in this room, who are advocates and members of civil society groups, deserve a huge amount of credit for all of the heavy lifting you've done on this front. FIPA, as well as the BCCLA, Open Media and others, continue to do stellar work on initiatives such as the stop online spying campaign, police information checks, and the current PIPA review to name just a few issues where you have brought privacy and access to the fore. Kudos to you also, for leading the charge to focus public attention on the issue of surveillance and national security. In my view, we need greater transparency, independent oversight and law reform at the federal level for national security agencies and their surveillance activities. You have helped illuminate the necessity for these changes.

I have been a regulator in other jurisdictions in Canada and I know just how lucky we are in B.C. to have a savvy access and privacy media, as well advocacy organizations and academic experts on the leading edge of information rights. This provides a powerful platform of strength that allows us to share with British Columbians just how important and relevant strong information rights are to everyday life. Citizens need regulators, advocates, and technology experts to ask the right questions, and push the discussion back to the fundamental privacy and access issues at stake. I think the ongoing coverage of these issues, and the advocacy and public education work of all of you in this room cues the public on how vital these rights are, and why we must vigorously defend them.

Given all of the matters confronting us—especially new technologies and new ways of doing business—I am often asked whether our existing access and privacy laws are sufficient to meet the challenge. On the privacy side, the answer is yes. Our laws are keeping up! Canada's privacy laws are comprehensive, and technology-neutral. And if we carefully apply a principle and value based approach, I think the laws are elastic enough to address the big challenges to privacy rights in the 21st century.

What do I mean by a principle and value based approach? First, there are the animating principles of privacy law such as notice, consent, openness, collection and use limitations and safeguards. These principles are based on the 1980 OECD guidelines and underscore all Canadian privacy laws. There are also the set of global values that underlie privacy rights and are fundamental to a fair and democratic society—human rights and the rule of law among them.

Even after several decades of privacy law, these principles and values remain relevant, still workable, and flexible in the face of the new "public" space of the Internet, cloud computing, big data and the Internet of Things. An ongoing challenge seems to be that some organizations, agencies, business and governments are forgetting these fundamental principles and values when faced with new technology.

We have to resist being blinded by shiny new technologies or we won't see the forest for the trees. It is imperative that we measure and implement new technology on the basis of our still very relevant laws. My office has taken this principle and values based approach to the more complex technical files to hit our desks. When we investigated ICBC's offering up of its facial recognition technology to the Vancouver police in the wake of the 2011 Stanley Cup riots, a principle and values based focus quickly got us to the heart of the matter—that access to ICBC's Facial Recognition Technology ("FRT") database by police was a change in use and not permissible without a warrant.

We applied the same approach to our investigation of automated license plate recognition—with a focus on what a law enforcement purpose was, and when that purpose is extinguished. We determined that a disclosure of non-hit data (license plates of citizens who are going about their lawful business) could not be disclosed by the Victoria police to the RCMP.

Both of these investigations were complex and involved new technologies. With a principle and values based approach, we were quickly able to cut to the heart of the matter and enhance the privacy of hundreds of thousands of people.

Advocacy groups are taking this approach too: shortly after revelations of mass surveillance by the NSA in the United States, the Electronic Frontier Foundation published *"13 Necessary and Proportionate Principles"* as their set piece for surveillance reform. Drawing heavily from human rights law, the 13 principles are the foundation for their calls for reform. The Principles have been signed by over 470 organizations and 350,000 individuals throughout the world.

Even the Supreme Court of Canada is getting in on this! *R v. Spencer* contains some of the most important and sweeping statements the Supreme Court of Canada has ever made about privacy—an indication of how seriously our top Court views the privacy rights of Canadians. The Court engaged in a fascinating discussion about informational privacy and, in particular how this privacy right extends to Internet use. Through this value based approach, the Court articulates the importance of what it called "privacy as anonymity" in the online context. This principle leads the Court to conclude that anonymity can be the basis for constitutional protection. This case undoubtedly strengthens the privacy rights of Canadians.

That is not to say that things are perfect. There are situations that certainly do test privacy laws and the regulators like me charged with applying them. Consider the ubiquitous use, and opaque nature of information processing known as big data. The oncoming tidal wave of data analytics in commercial, government and health contexts strain privacy principles of notice, openness and consistent use. However, it is still my belief that these issues are soluble by going back to basics, and the foundational values and principles that have guided our work thus far.

Having said that our privacy laws are essentially sound, is not to say they could not use a few tweaks. As many of you know, the legislature is currently reviewing BC's private sector privacy law, the *Personal Information Protection Act* ("PIPA"). Our Office has put forward four main recommendations for reform. The two big ones are: mandatory breach notification in the private sector—with notice to affected individuals and the OIPC in cases of real risk significant harm. In my view, mandatory breach reporting would increase private sector investment in privacy and security, level the playing field for organizations, and ensure our laws are harmonized across Canada. The second big recommendation is a call to end warrantless disclosure of personal information by BC companies. Section 18(1)(j) of PIPA gives broad authority for organizations to disclose personal information to a law enforcement or government agency without the knowledge or consent of an individual and without a warrant.

At present, companies have the discretion to comply with a request, or they can refuse to release personal information without a court authorized order. Many companies have told me that they refuse such warrantless requests; others may be less resistant to the request because of the broad language in this section. We have no way of knowing the number, scale, frequency or reasons of these kinds of disclosures. There are no provisions requiring organizations to report on them, and British Columbians seeking access to their personal information would likely find it difficult to even know if a company had disclosed their data.

Prior to the *Spencer* decision being released I raised the issue of warrantless disclosures with the Legislative Committee reviewing PIPA. I recommended (at minimum) that the law be amended to provide for transparency of disclosures made to law enforcement in the absence of a court order. However, in light of Spencer, it is arguable whether this provision is constitutional and should be deleted all together. I've also flagged the issue of the breadth of organization to organization disclosures referred to in s. 18(1)(c) in a subsequent letter to the Committee—and that concern has also been echoed in some of the public submissions made to the them.

While we didn't see any changes to the law as a result of the 2008 PIPA review, I'm optimistic we will see meaningful amendments to the statute as a result of the Committee's deliberations this time around.

Now turning to access rights. We have a legislated framework and as all of you in this room know that frameworks has faced challenges, and in particular I think of the lack of coverage of subsidiary corporations, a series of legislative carve-outs and notwithstanding clauses, and court decisions about advice and recommendation exemption. All of these matters require legislative fixes. However, what is even more crucial is for the government to fully inspect and bolster what is the very foundation of the information rights regime.

Here I refer to government's information management system—the way public bodies organize and keep records. That system is broken and in urgent need of reform. Good information management is the foundation of access rights. If there are no records of government's decision-making processes, there can be no openness. And when reams of records do exist there can be no ready and efficient access to them without proper record management systems. All of this results in a public trust deficit. Good information management requires standards for records creation, standards for records keeping and Rules for deletion and preservation. The entire lifecycle of a record should be covered, which is why I have been calling for comprehensive information management legislation.

Information management must include a duty to document, the key actions, deliberations and decisions of government. Civil servants come and go, but a written record of decisions made must endure if we want to preserve transparency, accountability and access to information. Without writing things down, the details of how and why a decision was made is forever lost.

All that BC has on the books is the 1936 *Document Disposal Act*, passed in the same year *Gone with the Wind* was published! An era when the photocopier wasn't even invented yet!

New information management legislation, whether contained with FIPPA or in a stand-alone act, also needs to address how government handles digital records. The BC Government needs a new system to file, organize and archive the countless digital records being created every day. A new system would make searching for records more efficient, and streamline the process of searching for records in response to business, legal and access requests. Other jurisdictions have modernized their records management legislation and policies to reflect the challenges of electronic records. And as we kick off Right to Know Week, I cannot emphasize strongly enough, how fundamental it is to access rights to fix this system!

It won't happen overnight. Instead of a *Document Disposal Act*, we need a *Records Keeping Act*—with provisions for a duty to document, for building access as a design element into new systems, for a digital records strategy, mandated archival provisions and independent oversight. This will go a long way to preserving the public's right of access in the years to come. I'll be looking for some help from all of you to do that. We need to keep government's feet to the fire in the access arena.

So, to sum up, I have laid out an ambitious agenda for reform amendments on the privacy side and big changes on the access side. I am both hopeful and optimistic as we journey down this road.

And I am so glad to be here with you to talk about these important issues. I wish you all a very good conference and hope to have a chance to speak with you throughout the day. If we have time for questions, I am happy to take them.