CHECK AGAINST DELIVERY

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

FIPA Information Summit

Commissioner Elizabeth Denham
September 19, 2012

Good morning. It's great to be here.

Thanks to Vince, Richard and the FIPA advisory board for the invitation to open the conference.

I see a lot of familiar faces in the room. My colleague and friend, Suzanne Legault, the Information Commissioner of Canada is in the audience. And of course Darrell Evans is also here. As some of you might know, Darrell has recently taken up a new challenge. He'll be leading the effort to create the Canadian Institute for Information and Privacy Studies.

I want to take this opportunity to recognize the professional and personal commitment Darrell has made to FIPA over the years, as well as his yeoman service in advancing access and privacy rights in this province, and across the country!

I'd also like to formally introduce Michael McEvoy – our new Assistant Commissioner for Policy & Technology. Most of you in this room are familiar with his cogent decisions and orders issued over the past five years in his role as adjudicator in the office. I'm delighted with his ascension in the office and I will rely heavily on his advice in his Assistant Commissioner role.

The last time I spoke at the FIPA information summit, I had been on the beat as Commissioner for about 90 days.

I delivered my maiden speech as Information and Privacy Commissioner to this audience. At that time, fresh from a few years in Ottawa, I told you I was feeling a bit like Dorothy in the Wizard of Oz…. not being in Kansas anymore and all that.

I leave it to you to decide whether I fit in with all of you by now!

Vince wanted me to share with you some of the things we've been up to in two short years. Simply stated, it has been a CRAZY time of whirlwinds and a few tornadoes!

I try to tell the staff that protecting access and privacy rights is a MARATHON, not a sprint, but in truth, we've set a new **race pace** for this office. Thankfully, we now have more of the resources we need to provide effective oversight.

The Legislature granted my office budget increases in each of the last two fiscal years, most recently to address an expanded mandate as a result of amendments to BC's public sector law.

Our most recent budget lift allowed us to hire three new policy analysts – this increased capacity has been critical as we review mandatory Privacy Impact Assessments for integrated programs of government, and as we keep tabs on new data-sharing projects facilitated by the amendments, including the new BC Services Card.

We've also hired a Manager of Communications and Public Education, and a Technical Investigator.

In addition to having a few more bodies around the office, we've shuffled staff assignments to allow us to do more proactive work on the broader policy issues affecting information rights.

I wanted to increase the capacity of our office to be more forward-looking, and better able to tackle some of the bigger privacy risks on the horizon.

We now have two teams – investigations and mediation, who work to resolve complaints and inquiries coming through our front door… and Michael's group whose focus is systemic investigations and proactive reviews.

In the past year, our policy team completed six Commissioner-led investigations, and initiated four more, including: BC Hydro Smart Meters, ICBC's use of Facial Recognition Technology, a privacy breach at the University of Victoria, and the BC Government's use of criminal record checks in the hiring process.

And – coming soon – of special interest to you and to the open data panel later this morning: an audit on BC government's open information/open data program. Also coming soon is our review of public interest disclosure practices (section 25) and a report on Victoria Police Department's use of automated licence plate recognition. So stay tuned.

Another area that I've been very focused on over the past two years, is building our office's capacity to address the impact of new and emerging technologies on privacy – everything from social media and mobile technology to the new data-sharing and e-health initiatives underway by government.

Our office is very much alive to the privacy and security issues inherent in these technologies. And we know that citizens, consumers, and companies are looking to us for guidance on how to ensure that privacy and technology are **complementary** values, not **competing** values.

We've also published new guidance to give public bodies and businesses some best practices to follow as they dive into these technologies.

For example, we published guidelines for employers on conducting social media background checks, an interactive security checklist for businesses, and cloud computing guidelines for public bodies and the private sector.

My third key priority since taking office is to enhance our public education and outreach. Last year we increased our speaking engagements by 80%, delivering 90 presentations to public and professional audiences. We increased the numbers of op-eds and open letters.

You may have noticed that earlier this year I wrote a series of letters to the Legislative Assembly regarding Bills that I believe undermine British Columbians' access and privacy rights.

The most egregious Bill in my view was the *Animal Health Act*, which would have removed the public's right to access records regarding animal testing and animal disease management.

The Bill was not passed in the last sitting and the fate of this legislation is uncertain. My letter initiated public debate and discussion about the importance of access and privacy legislation.

My concern with this Bill, and also with *the Emergency Intervention Disclosure Act* and the *Pharmaceutical Services Act* was with overrides that frustrate the purposes of FIPPA and threaten to undermine the balance so thoughtfully and carefully articulated by legislators 20 years ago.

I've also joined my federal and provincial colleagues to express my deep concern about a federal Bill, Bill C-30 – the government's on-line surveillance Bill aka "lawful access".

Advocates and commissioners were successful in at least stalling this Bill, and we are hoping that parliamentarians will debate and reconsider its sweeping powers for law enforcement to access our personal communications without judicial oversight.

We're also in the process of revamping our online presence, to meet the changing needs of our stakeholders and to account for how they prefer to receive information from and about us.

Our office has entered the social media world, we're now on Twitter – you can follow us at @BCinfoprivacy – and next month we will be launching a revamped website – with improved content and functionality. So look for it very soon.

I hope this gives you a bit of a flavor of the pace and focus of my office over the past two years.

Looking back, it's amazing to see how far we've travelled. I'm proud of the progress we've made. I am supported in this work by dedicated and passionate staff, and by my external advisory board who has provided me with sound advice and guidance.

And of course I want to recognize the contributions of our fellow travelers in this room… who have partnered with us, who have challenged us, complained to us, and who work hard to put access and privacy issues on the front burner and on the front page.

FIPA is one of the best examples of that kind of public interest advocacy at work. You play a vital role in contributing to the terms of the debate, and the public dialogue and public interest.

As you can imagine, I spend a lot of time in rooms like these talking about the value of privacy and freedom of information. I'll admit that sometimes it feels a bit like preaching to the converted. For example, when the Privacy Commissioner is invited to a privacy conference to talk about the importance of privacy with an audience who thinks these rights are important.

But then there are times when you are invited to attend a meeting, or speak at a conference about access and privacy, and you start to have a conversation with a group of people about the issues.

You ask them questions about protecting privacy in a networked world, and you get people thinking a bit more critically about the cloud and what's in it. Or, you start talking about the opportunity around opening up information about government through proactive disclosure and open data. And you get an incredible amount of engagement and *energy* and *passion* in the room!

Now we don't always agree. But we're having a discussion, a debate, about issues in access and privacy.

These moments are among the best in my job. And among the most important. Why? Because when we critically engage the public, and give them the straight goods about how their information is being collected, used, disclosed and secured, we give them the raw materials to engage in informed debate and to make up their own minds about what to think and what action to take.

As a regulator, I believe that we have a HUGE role to play in promoting that understanding and dialogue. The onus is on us to **pull back the curtain**, to shine a light onto the far corners of a program, policy 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 detailed and systemic investigations. When we exercise that authority, we dive deeply. We inspect every relevant detail of a new or existing program, activity or policy. 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 assess compliance.

But we also have a public education mandate. Not every Commissioner has one. Education and enforcement might seem like divergent responsibilities. But in reality they are two sides of the same coin.

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 results of our investigations when it is in the public interest to do so.

That's what made the federal privacy commissioner's Facebook investigation so ground-breaking. It wasn't just the findings in the case, it was the first time that a regulator had laid bare Facebook's business model, how the platform actually worked. Up until that point, people looked at Facebook as primarily a social platform. As a result of that work, and the efforts of others in the privacy world, people started to see Facebook as a marketing platform. They started to advocate for change. Consumers' voices are extremely powerful.

There is no guarantee that in publishing these details… that the public will necessarily agree with our findings. They certainly will not see us on the side of the angels in every case.

They may decide that despite what it might mean for their privacy, that they want the latest shiny new toy that sends packets of geo-location data and web surfing habits to the cloud. That trade-off is acceptable to them. Or, citizens might demand that their government abandon plans on a major initiative or surveillance scheme.

And that's how the system should work. Citizens and consumers choosing, or taking action based on an ***informed*** choice on transparency. They are taking control of their personal information.

This is precisely why we're investigating ALPR. Why we're inspecting the government's open government initiative. Why we're reviewing the Integrated Case Management system as it's being built.

Now, just before I conclude my remarks, I need to take you back to Kansas. In one of the last scenes of the Wizard of Oz, Dorothy and her friends arrive at the end of the yellow brick road and unveil the wizard's true identity. At that moment, a voice from above bellows, "Pay no attention to the man behind the curtain!"

There will always be those who will take the wizard's advice – not to look behind the curtain, not to question what is happening with their information or the effect an organization's practices have on their privacy….

But what we MUST do, as regulators, advocates, academics and members of the public… is continue to shed light on those issues of access and privacy that truly matter to British Columbians, so that citizens can make informed choices, OR advocate for change.

All of us will continue that work. We have to keep the dialogue, the debate going. British Columbians are looking to all of us in this room for leadership. I am confident we will not let them down.

Thank you for your kind invitation to address you once again. I look forward to the panels and speakers, and to chatting with you throughout the day. Enjoy the conference.