Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

Commissioner Elizabeth Denham's Keynote Address to the 13th Annual Privacy and Security Conference Victoria, British Columbia February 17, 2012

Privacy, Accountability and the Digital Revolution

Thanks to all of you for being here this afternoon. It's always a pleasure to come to Reboot.

It's one of the few places where you have techies, security experts and policy wonks in the same room talking about the technology that's changing our world.

You have to admit, it's a pretty cool place to be. Although sometimes, I think maybe I'm not quite cool enough for this conference. Let's face it: I'm not exactly Steve Jobs.

But sometimes I wish protecting privacy was as easy as downloading an iPhone app.

I can see it now…You're on a smart phone, keying in banking information on an unencrypted connection. Or maybe you're on Facebook, posting some juicy details about the Reboot hospitality room last night. When all of a sudden…a message pops up on your screen.

"Warning! Warning! Your privacy is at risk!"

OK, so maybe smart phones can't do everything. But maybe someday… someone will come up with an app that can do some of these things.

So, I'm not Steve Jobs. But I **am** the Information and Privacy Commissioner for B.C. And I'm very proud of the work my office has been doing in the space where privacy and technology meet.

I want to share some of that work with you today. But before I begin, I want to put some things into perspective.

This year marks the 20th anniversary of the BC government's access and privacy legislation. Most of us didn't know it at the time…but we were on the verge of a digital revolution. And while the companies leading that movement were making (what turned out to be) accurate predictions about the technologies of the future…they couldn't predict how these technologies would transform our lives. In some ways, it's getting harder to imagine – or remember – what life was like before the shift.

Take 1993, the year the Act came into force. In June of that year, there were a total of 130 sites on the web. Think about it: You could visit every single website in a SINGLE DAY! And thanks to a new web browser called Mosaic, we could "see" those 130 web sites in graphic format, instead of just reading line after line of text.

The Whitehouse had two email addresses: president@whitehouse.gov and vice-president@whitehouse.gov. And the newest gadget was the Apple Newton MessagePad, an early version of the tablet, with handwriting recognition so bad … you could barely use it. (Let me put it this way. If I had written this speech on the Newton, I'd be in big trouble.)

In 1993, our Office was setting the groundwork for information and privacy in B.C. The lion's share was on the access side of the ledger – mediating requests for review, adjudicating FOI disputes, and so on. But we did deal with some interesting issues in privacy and technology.

We investigated the security and privacy controls for a new, province-wide e-health network called BC Pharmanet. And we commented on a proposed data sharing program, where Ministries and public bodies, in B.C. and other provinces…would match up data tapes to identify double-dipping citizens.

These were pretty cutting-edge for their time, pushing the boundaries of our expectations. But they are nothing compared to the changes we've seen in the last 20 years. Fast forward to today, were one-third of the world's population is online.

We send 294 billion emails and 250 million tweets a day. And as the size of our online world expands from gigabytes, to terabytes, to zettabytes…the number of people and technologies seeking to mine that data is growing just as fast.

Our challenge is how we make sure privacy is inherent in the systems we create to manage and manipulate all this data. Some believe that the solution is to design shiny new systems with all the bells and whistles built in to protect personal information.

This is important of course, but it misses the mark. Why? Because privacy is not an add-on, or an upgrade. Nor is it just a lens we apply only when we build new data systems or new offerings… or transfer data across borders. Privacy must be part of an organization's DNA. Personal information must be accounted for and managed … before we start designing those systems. The real solution is for organizations to create privacy management programs that will underpin all new systems that touch personal data.

Today, I want to talk about how my Office is working to get public and private organizations to invest in privacy management…before they design and apply new technology.

When I first took over as Commissioner's in 2010, the office was structured to deal with issues reactively. If there was a privacy breach, we could investigate. If personal information was being misused or mishandled, we could look into it and order changes. This approach helps individual complainants, and can provide retrofits and program changes ….after the fact. But it doesn't address, for example, the increasingly obscure and opaque nature of 21st century data processing.

These days, how do people even know what to complain about? And a reactive approach, focused on single, technical breach of the Act……doesn't set up organizations to manage future risks and incidents. Kind of like chipping away at an iceberg, without peering into the ocean below.

So last year, I reorganized our staff into two teams – an investigative group to address the complaints and inquiries coming through our front door…and a policy and technology group whose focus is systemic investigations and proactive reviews.

In 2011 we published three Commissioner-led investigation reports, and initiated two more. These investigations go beyond the surface issues and technical

compliance. They provide guidance to organizations about how to strengthen their privacy management programs.

Let me share just a couple of examples with you.

Smart Meters

BC Hydro is currently installing smart meters across B.C. Once fully functional, smart meters will collect energy usage data on an hourly basis and transmit it wirelessly to B.C. Hydro. This data provides more granular information about us. Enough detail to know, for example, when we are at home and away.

There was a compelling public interest for my Office to investigate the privacy and security aspects of smart meters. We found that Hydro failed to notify its customers about the information it was collecting through this new technology, in accordance with BC privacy law.

The importance of notification cannot be overstated, especially when new technology is involved. But we also took the opportunity to examine the foundational supports – the people, the processes and the data management practices in place at BC Hydro.

Not only did we ask, "Is Hydro complying with privacy laws in smart metering?" But also, "Do they have responsible information governance?" "Does Hydro have the capacity to implement security and privacy controls, whatever the project?"

We made 13 recommendations to address Hydro's privacy management program.

We recommended role-based access… to restrict employee access to customer information on a need to know basis. We recommended that Hydro appoint a person responsible for privacy, who would either be a member of the executive team or a key person at the decision-making table. And we recommended better record retention and disposal policies, so the company does not hold onto customer information indefinitely.

BC Hydro agreed to address all of our recommendations.

Facial Recognition

Our most recent investigation started with a hockey game.

In the hours after Game 7 of the Stanley Cup final, hundreds of people committed acts of vandalism and looting in Vancouver's downtown core. British Columbians demanded swift justice. And in response, ICBC offered to check

images of alleged rioters provided by Vancouver Police against its facial recognition database.

Facial recognition measures the biometric details of a person's facial features, and uses them to create an algorithm that represents that person's identity. It's a digital imprint of our physical selves.

Our investigation was three fold.

First, we looked at whether ICBC's internal use of facial recognition complied with public sector privacy law. We found that while the purpose and compilation of the database was compliant, there was insufficient client notice. Most British Columbians didn't know facial recognition was in use at ICBC to detect and deter driver's licence fraud. And they were disquieted by the fact that they learned about it through the media rather than from ICBC. Again, with new technologies, proper notification is essential and required by BC law.

Next, we examined ICBC's offer to match external images of rioters against its driver's licence database. Many people's spidey senses were tingling here – and indeed we found that this data matching amounted to a change in use of the personal information…and was not authorized under the Act – even without disclosure of the match to police. This kind of data manipulation, especially when it involves biometric data, requires a court order or subpoena. Judicial oversight. Full stop.

Finally, we looked at ICBC's overall privacy management program. While we found sound security and information policies, ICBC needs to better communicate accountability throughout the organizatio*n*. For example, the Privacy Manager was not consulted about ICBC's offer to the Vancouver police.

ICBC has agreed to strengthen privacy governance in the wake of our report.

With technologies like facial recognition and smart meters we have set the bar very high…because of the potential future uses of these technologies and the inherent risks to privacy. These systems collect very detailed and very sensitive information about us. And they aren't even fully developed yet.

That's why it is so critical to have strong data governance.

Data Sharing

I want to change gears and talk briefly about data-sharing.

Amendments to the Freedom of Information and Protection of Privacy Act, passed last October…give public bodies expanded authority to share personal information between agencies for common programs. Also under the

amendments, government bodies can link information between databases. But they will have to follow strict rules to ensure personal information is protected.

Data sharing and data linking schemes undertaken by government now require detailed privacy impact assessments…submitted to my office for review and comment.

We will soon be issuing Guidelines so that you know what to expect from us when you submit a PIA.

Identity Management

The amendments also create an identity information management service that will pave the way for secure online government services. BC is the first Canadian jurisdiction to venture into this very challenging and complex area of IDM. But we have to get the policy right.

BC's "claims based model" which federates credentials is an acceptable model to some privacy advocates. But it's another example of that shiny new system approach…where we must not lose sight of the fact that the policies, practices and people must be in place to ensure privacy is managed BEFORE design.

Taken as a whole, these amendments create a shift in oversight, and are a real opportunity to encourage a culture of privacy…where the foundation is laid and responsible practices exist across public bodies.

They also mean new responsibilities for my office. We are hiring a new team of technical analysts. Check our website for job postings!

Accountability Tool

Finally, I want to bring to your attention to the work our office is doing to put the tools in your hands…to create comprehensive privacy management programs.

Back in 1993, Commissioner David Flaherty could be pretty persuasive when he dropped by for a site visit. I don't make many house calls these days. But those of you who know us best, have probably experienced a breach, a complaint about your practices, or some other incident that attracted our attention.

We will, of course, continue to respond to these privacy incidents – certainly a major data breach can move the marker in one organization and its closest peers.

But we need to shift the use of our resources, maximizing the incentives and providing the tools for good data governance. The bottom line is accountability.

Organizations, public or private, that collect personal information from their customers and citizens…assume legal and ethical responsibility for privacy protection. And they should stand ready to demonstrate to citizens, customers, and to Privacy Commissioners in the event of a complaint, investigation or audit…that they have the right policies, breach protocols, privacy training, and security to address privacy risks. We are looking for actions that show a commitment to a culture of privacy, not just the "paperwork of privacy."

That's why my office, in partnership with Jennifer Stoddart's Office and with Jill Clayton's Office in Alberta, developing what we are calling an Accountability Tool. I'm really excited about this. And here's why.

I suspect that for many of you, defining what "effective privacy management program" means is like nailing jelly to a wall.

This guidance document…called **Getting Accountability right through Privacy Management Programs**… signals the end of guesswork. It lays out a blueprint for a privacy management program.

We're focused on the private sector at this time, but this document is equally relevant and useful for public bodies. And because privacy is ever changing – especially in the face of new and emerging technologies, evolving jurisprudence and industry best practices...we've made regular review an essential part of the program.

Privacy isn't a project. It's not a one- time compliance exercise. It's a dynamic process. And it isn't bullet proof. There will be times when mistakes are made.

But with a solid program, you will be able to identify vulnerabilities, strengthen your practices and promote a culture of privacy throughout your organization.

Our Accountability Tool will be published in the coming weeks. We've been consulting businesses and experts to get their input. Look for it very soon.

Lawful Access

In closing, I want to leave you with a few comments about a critical issue that is top of mind for me and for privacy commissioners across Canada:

Bill C-30, the Investigating and Preventing Criminal Electronic Communications Act aka Protecting Children from Internet Predators Act.

As most of you know, the Bill is a re-incarnation of Bills C-50, C-51 and C-52, which died on the Order Paper when an election was called last year. If there was ever a piece of legislation or current event that showed the connection between technology and privacy… this is it.

The intent of the Bill is to provide new authority for police and national security agencies to access our electronic communications…in some cases without judicial oversight, in other cases, with a lowering of evidentiary standards.

Privacy Commissioners across Canada speak with one voice on this issue.

This is an unprecedented and unjustified erosion of Canadians' privacy rights.

The latest news is that Bill C-30 has been referred to a Committee for review, before it is debated in Parliament.

We are cautiously optimistic that through study and scrutiny…Members of Parliament will find a way to preserve Canadians' fundamental right to privacy and autonomy.

Privacy Commissioners will continue to raise our concerns. And we will continue to advocate for a framework that includes transparency, judicial scrutiny and robust oversight.

But what is really needed… is for citizens to take up the charge! I encourage each and every one of you to inform yourself about these proposals. If you have concerns about lawful access, now is the time to find your voice. Phone or write to your MP, or join the list of thousands of Canadians who have signed the Open Media petition on this issue.

You might think that a single voice doesn't matter. But it does. Citizens made the difference in the United States, when we saw a groundswell of opposition to SOPA legislation. Perhaps there is an opportunity for a SOPA-esque moment here in Canada, too.

So I leave it with you today, to contemplate how you feel about these proposals, and how they might affect your rights. And I encourage you to know your rights and to get involved.

Thank you for your attention this afternoon.