Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

PROTECTING PRIVACY IN A CONNECTED WORLD

Elizabeth Denham
Information and Privacy Commissioner for B.C.

Keynote Presentation to the
14th Annual Privacy and Security Conference
Victoria, British Columbia
February 8, 2013

Good morning everyone. It's a pleasure to be here.

Let me first thank Richard Purcell for the introduction and to the Office of the Chief Information Officer, and also Greg Spievak, Carla and the team at Reboot for organizing such a wonderful conference.

All of you here today realize that there is a very special community here, and I am grateful to be a part of it!

My remarks today are supposed to be about what's on my desk, the work of my office. But instead, I want to use this time to talk about how our connected world has changed the way we create, use, collect and share information, and what that means for our privacy rights.

I'm starting here because many of us assume that technology, the Internet, and social networking are the primary forces shaping our relationship to data. And, while it is true that these technologies do play a leading role, I think it's important we critically examine the "how" and the "what" of this shift. Because 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.

It raises questions about what privacy looks like today, and what actions we must take to protect it. I will talk more about that later. But first, let's explore what we know about how these technologies are shaping the landscape of our lives.

I think there are three major developments worth noting for the purposes of our conversation.

- **First, our relationship with data has changed.**

As a society, we have always been active consumers of information. The growth of internet technologies, Wi-Fi, and mobile devices has increased our collective appetite for data—from active to voracious.

These developments have also changed the way we interact with data. We've all become mass contributors to the information available online. 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.

This bi-directional mode of communication creates new possibilities but also new risks. We have gotten used to providing information online—much of it personal information. Most of us are shopping on-line, banking, dating, and gaming on-line. We've come to expect more services—including government services—at our fingertips.

All of these require a certain amount of personal data to be shared—which raises important questions about data security and how that information is being protected. That's the first development. Our relationship with the data has changed.

- **The second is that new technologies collect information about us that was not previously quantifiable. And a lot of it is personal information.**

This is particularly true for social networking.

We post to our timelines on Facebook, check in on Foursquare, share Flickr photos, and connect on Twitter. We trust these technologies with the stories of

our lives. And each and every one of our stories can now be quantified, and monetized.

A backyard conversation with your neighbour about where to take your next summer vacation could not previously be leveraged by marketers. But if you have that conversation on Facebook or Trip Advisor… well, that's a different story.

The *Wall Street Journal* estimates that companies whose business depends on collecting personal information and using it to attract advertisers is worth nearly $30 billion dollars. This phenomenon is not exclusively in the online domain.

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 right here in BC 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—a development that's not been lost on the public.

Which brings me to my third point.

- **And that is the tension between the public desire to leverage these tools––and public concerns about the fate of privacy in the wake of these technologies.**

There's no question that we want a customized user experience, we want to make the routine or mundane tasks in our lives to be quicker, and more efficient. We also have a desire for connection.

These tools and technologies have the potential to meet all of these needs, but there is also an acute awareness and concern about the privacy risks.

A study released in 2012 by McLaren McCann shows that privacy is very much a top-of-mind issue for Canadians. Nearly three-quarters of Canadians identified themselves as "concerned" or "very concerned" about the erosion of their personal

privacy. I'll say it again: Almost 75% of Canadians are concerned about the erosion of their personal privacy.

Our fears about privacy are second only to worries about the global financial crisis, and have surpassed climate change, terrorism and all of these other issues that we see in these 'most important problem' type polls.

The pollsters wanted to delve deeper into the "why" of these concerns. They wanted to know what societal trends were shaping these concerns about privacy.

They found two major contributing factors. Guess what they were? Technology and social networking.

All of this begs the really big question, which is:

> *How can citizens trust that their personal information and is secure and protected and that their privacy is valued, in this connected world?*

The solution is not to turn back the clock on these technologies. Nor should we!

I love my iPad. I love Skyping with my far flung kids. I even used Google Street View to show my 80 year old father an image of the house he grew up in. These tools and technologies are clearly valuable to all of us.

But, citizens, consumers, and companies and governments need guidance on how to ensure that privacy and technology are complementary values, not competing ones. We know that privacy legislation plays a critical role. It is imperative that we have a robust legal framework and dynamic oversight. We may very well need new regulatory tools – including breach disclosure requirements, binding guidelines and administrative penalties. But there is more we can do with the oversight tools we have now.

Today I'm going to talk about three things privacy regulators can do to help protect privacy in this connected world.

- **The first is to use our regulatory powers to promote debate and dialogue about privacy––by providing citizens with detailed information about how these technologies actually work.**

This is a strategic investment of scarce resources in the fast-moving world of data protection.

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.

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.

This is precisely why we chose to investigate ALPR use by police. Why we examined ICBC's use of facial recognition technology. And it's why we are deeply engaged in inspecting the government's new BC Services Card program.

Most of you in the room know that the BC Services Card is launching next week. Later this morning, I will be making public my comments about our review of the first phase of the BC Services Card. You may hear news reports about it later this afternoon.

From my vantage point, I do have some concerns about the first phase of the program, but it is the next phase—which gets us closer to the world of online government services—that requires even more searching examination.

It is the government's ability to architect the system to prevent fusing and tracking of data about citizens' discrete activities that is of most interest to me. And we know those who are designing the program are also well aware of the need to get it right.

My big message to government is about the need for public engagement as it takes the next step forward—transparency and accountability and trust. Not a surprise, a theme that we have heard throughout this conference.

When we pull back the curtain, there is no guarantee that the public will necessarily agree with our findings. 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.

That's the first thing regulators can do.

- **Second, regulators must collaborate with data protection authorities in other jurisdictions to better promote and protect privacy rights.**

While privacy laws are bounded by jurisdiction—the value of privacy, and the data itself, knows no borders. No law, no privacy commissioner's decision or action exists in isolation.

Privacy commissioners increasingly collaborate in policy and enforcement work. Just last week, we saw the Office of the Privacy Commissioner of Canada and the Dutch Data Protection Authority release the results of their joint investigation of WhatsApp—a silicon valley based mobile app found to have significant privacy concerns.

Here in Canada, Commissioners from the provinces and territories often work together to take action on issues of collective concern. For example, we have taken a unified stand against the internet surveillance legislation (Bill C-30) currently before Parliament. I was before you last year, speaking about this Bill shortly after its introduction. Well it's back in the news again! And our concerns about the access to subscriber data without a warrant or judicial oversight continue unabated. And we continue, in unison, to raise our concerns about this Bill.

In addition to the collaboration within Canada, my Office is reaching out beyond our borders to participate in international privacy enforcement activities. BC is an active member of the Asia Pacific Privacy Authorities group, which includes enforcement agencies in Hong Kong, Australia, South Korea, Mexico, Macau, and the United States. We recently wrote a joint letter to Google regarding concerns about the company's privacy policy.

BC also recently became a member of GPEN, the Global Privacy Enforcement Network. We are currently working on a collaborative project with our GPEN colleagues to promote transparent privacy practices online. Stay tuned for that later this spring.

- **The third thing regulators must do is to take a pragmatic approach, with a focus on practical tools to assist public bodies and private organizations comply with privacy laws.**

Most of us in the room live and breathe privacy and security. We've drunk the Kool-Aid. But we can't forget that to the average person or business out there, it can all seem pretty overwhelming.

My office has a responsibility to educate, inform and provide practical tools to get those people and businesses from a place of feeling overwhelmed by all of the perceived requirements—to a place where they feel confident about compliance—and that benefits everyone. I'm quite proud of the work that we've done in this area.

In 2012, Canadian Commissioners responsible for private sector privacy jointly published guidance called *Getting Accountability Right*, which gives organizations practical building blocks to implement privacy management. Stay tuned for a companion document for the BC Public Sector.

We've also published guidance on cloud computing for public and private organizations, laying out the issues and the risks.

For businesses we developed a privacy policy workshop, with templates and tools to make it easier to develop a culture of privacy.

And for the public, we have a new website that breaks down some of the basics for those who are struggling to understand how the law works and how it affects them.

I believe that these small, practical steps get better results in terms of education and compliance.

All of you in the room are in the privacy and security business. You can lead by example. We know that effective protection of personal information is critical to public confidence in government, to consumer confidence in your business.

Build a privacy program to ensure that privacy is protected across your organization – so that every new project and every application starts with a privacy-positive foundation.

I want to leave you with a bit of shameless advertising for a conference my office is hosting later this year in Vancouver.

The conference is called Privacy and Access 20/20 a new vision for information rights.

This event will mark the 20th anniversary of the *Freedom of Information and Protection of Privacy Act*. It is a celebration of where we have come from and where we are going in information rights in this province and beyond. I hope to see you there. Reboot is assisting us in delivering the conference.

Thank you very much for your attention this morning and enjoy your day.