Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

SPEECH TO THE

TRU LAW STUDENTS CONFERENCE

FEBRUARY 4, 2015

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER FOR BC

Thank you for inviting me to be here today.

This is my second official visit to TRU since becoming Commissioner.

I was last here in May 2011, just before the law school opened its doors to welcome its first cohort of shiny new law students.

Today, those students are getting close to finishing their articles, the Faculty has moved into spacious (and stylish) new digs, and you have an impressive array of privacy law experts as part of your faculty.

You are fortunate to have David Hughes, and of course my predecessor David Loukidelis, as part of the faculty and sessional staff.

You may find this surprising but I was “this close” to becoming a lawyer.

I studied history and political science in the 1970s at UBC, and on graduation, applied and was accepted to law school to fulfill my dream of becoming a human rights lawyer – a career that would have fulfilled my passion for social justice issue and the interplay with the legal system.

But it wasn’t meant to be.

I know I disappointed my parents, by accepting instead an offer to pursue graduate studies in information science in the newly-minted Master of Archival Studies program at UBC.

I followed my heart into the world of preserving and overseeing access to archives and historical records, something I believe you would all agree was at least as sexy as the world you are entering.

And it launched me head-first into a fascinating career.

After graduating from UBC I worked as a City Archivist in my hometown of Richmond and Calgary, and then, after the passage of new access and privacy laws in Canada – as a privacy officer for a health authority, a privacy consultant, and finally as a regulator enforcing privacy laws in Alberta, Ottawa and now in British Columbia.

Really there is no end of possibilities in the jobs and careers you will enter in the years ahead. Being flexible and open to new possibilities is key. I certainly didn't expect to be in this role when I was a graduate student.

I was appointed B.C. Information and Privacy Commissioner for a six-year term in 2010. I'm extremely fortunate (and never expected) to be playing a policy and regulatory role at the intersection of privacy and technology in the internet age!

Before I delve too deeply into the topic of privacy law in the digital age, I first want to describe the Commissioner's role and the activities of my Office.

While some of you have studied privacy law, and some of today's sessions today dealt with privacy matters – some of you may not be familiar with my Office and what the Commissioner actually does.

Commissioner's Overview

The Information and Privacy Commissioner oversees and enforce two different privacy and access statutes – one for the public sector and one for the private sector.

The Commissioner is an Independent Officer of the Legislature, which means I report to the Legislature as a whole, and not to Cabinet or a Minister.

This is important because it gives me the independence to oversee the privacy and access to information practices of government without accusations of partisanship or a perceived conflict of interest.

BC's public sector privacy and access law applies to every public body and agency you can think of -- 2,900 public bodies across the provincial, health, and local government sectors.

The scope of our private sector law is also sweeping. It applies to more than 380,000 organizations – including businesses, non-profits and, uniquely to BC, to all provincial political parties.

My job is to make sure that state and commercial actors are compliant with privacy law in their everyday practices.

It is also my job to educate the public about their access and privacy rights, and to make public comments about proposed laws, policies, programs or systems that have an impact on personal privacy.

If a member of the public has concerns about an organization's practices, I have the power to investigate.

Every year we investigate about 500 complaints and receive 650 requests for appeals under access to information law. We are the appeal body for responses to freedom of information requests.

I also have the authority to initiate investigations on my own motion, absent a complaint. We most often choose files that deal with the complex intersection of technology and privacy. Often times technology is so complex – that individuals do not even know what to complain about.

Privacy and Technology – FRT

For example, in 2011 I initiated an investigation into ICBC's use of facial recognition technology.

Facial recognition scans a photograph or a video image of a person's face, and creates an algorithm as unique as a fingerprint to identify that person.

We call this biometric data, because it measures unique characteristics of the human body – like a person's face, DNA, retinas or irises. By its very nature biometric data is incredibly sensitive.

At the time, ICBC was using facial recognition to detect and prevent driver's license fraud – for example by cutting down on the number of people that get duplicate driver's licences under different names.

In June of that year, Vancouver hosted Game 7 of the Stanley Cup Final. And we all know what happened next.

In the wake of the Vancouver Riots, ICBC made the police an offer: if you provide us with photographs of alleged rioters, we can use facial recognition to match them against photographs in our database.

Before the police commented on this offer, I initiated an investigation on my own motion and looked at how ICBC was using facial recognition software and whether it complied with BC privacy law.

Our investigation reviewed and revealed the extent of ICBC's FRT program, and we found that while ICBC was authorized to use facial recognition to detect and prevent fraud, the company had failed to notify customers.

We also concluded that under our privacy law, police are not allowed to use ICBC's facial recognition software without a court order. There also needed to be judicial authorization for every search of the biometric database.

With this investigation, we were able to explain to the public in plain language what ICBC was doing with this technology, and we made important recommendations to make the corporation more transparent, including notifying the public that it was using facial recognition.

I tell you this story because it illustrates the challenges of privacy and technology and why independent oversight is so important.

We can probably all agree that technology is, for the most part, making our lives easier and more efficient.

But we, as citizens and customers may not see the whole picture: including the ways state and private actors are using their personal information, for what purpose, and whether that use is lawful.

It is my job as a regulator is to pull back the curtain, to show the public what they know, and maybe what they don't know, about the privacy implications of the technologies that control our lives and interactions with government, industry and in our personal lives.

Privacy, Social Media and Facebook investigation

Of course, when we talk about privacy and technology most people's minds go immediately to social media.

Social media is a huge part of our daily lives.

And there is a lot of concern about how people are using information we post to social media and whether we have privacy rights when using these tools.

I am here to tell you that you do have privacy rights on social media.

Privacy Commissioners have defended this right in several ways over the years.

For example, here in British Columbia we've made clear that employers do not have the right to ask you to hand over your social media passwords.

Even without a password, checking out job candidates on social media sets employers up to collect a large amount of information that is potentially inaccurate, and likely in excess of what would be needed for a hiring decision and what would be authorized under privacy and human rights law.

And Canadian privacy Commissioners have taken on social media giants directly… to hold them to account under our comprehensive privacy laws.

Case in point: When I was Assistant Privacy Commissioner of Canada, I led that office's investigation of Facebook's privacy practices.

How does a Canadian privacy regulator take on a Silicon Valley internet giant like Facebook?

The short answer: a timely complaint, and legal authority to investigate… even though Facebook isn't headquartered in Canada.

In 2008, the Privacy Commissioner of Canada received a detailed complaint from a group of law students from the University of Ottawa – from the Canadian Internet Policy and Public Interest Clinic.

This was the most comprehensive and detailed complaint ever received by that Office. And it was the first complaint to any data protection regulator about a social media platform.

This investigation was a "first" in many other ways for the office. Historically, privacy complaints had mainly concerned Canadian-based brick and mortar organizations, not US- based companies operating entirely on-line.

However, the federal court previously ruled in *Lawson v. Accusearch* [1] that if a company has a "real and substantial connection" Canada had an obligation to comply with our privacy laws and the federal Privacy Commissioner has jurisdiction to investigate complaints relating to the transborder flow of personal information. That was our way in.

Our investigation was exhaustive and resulted in a report of more than 100 pages and some important changes to Facebook's privacy practices, including a reconfiguration of its platform to ensure third party apps could not scrape data without users' knowledge and consent, and the first iteration of privacy controls and transparency tools.

[1] Lawson v. Accusearch Inc. (F.C.), 2007 FC 125, [2007] 4 F.C.R. 314

It took about a year, but Facebook complied fully with the Office's recommendations, keeping the complaint out of the courts. It also applied its changes globally, not just to Canadian users.

After we published our investigation report, with all the nitty gritty details of how Facebook worked behind the scenes, many technology experts and media leveraged the report's findings to educate the public on Facebook's business model, the fundamental role personal information plays in Facebook's ecosystem.

Privacy, Technology and State Surveillance

Of course, we can't talk about privacy and technology without considering intelligence gathering of Canadians' online activities.

Informational surveillance – the digital crumbs about our on-line activities including internet search history, emails, and file transfers is keeping privacy commissioners up at night. And the public is also concerned.

Just last week, documents came to light that show that Communications Security Establishment Canada – our signals intelligence agency called CSEC – is using a program called Levitation to track up to 15 million downloads to file-sharing programs PER DAY, acting on behalf of the "five eyes" surveillance sharing programs (Canada's partners are the UK, Australia, New Zealand, and the US).

And last Friday the federal government tabled Bill C-51, the proposed new national security legislation. The Bill provides broad new powers for CSIS, CSEC, and law enforcement agencies in response to horrific attacks experienced in Ottawa, and in Saint-Jean-sur-Richelieu Quebec and elsewhere.

These new powers make it easier to detain suspected terrorists, enhances the powers of CSIS to disrupt threats, criminalizes advocacy and promotion of terrorism, and makes it easier to government to share national security information.

We all acknowledge that security is essential in maintaining our democratic rights. But I'm deeply concerned that these new measures are not designed in a way that protect freedom of speech and privacy.

To give just one example – the Act seems to allow federal departments and agencies broad new authority to share personal information, including information of Canadians not suspected of terrorist activities, for the purpose of identifying new threats.

This kind of broad sharing is a privacy game changer. It is not clear whose information will be shared with national security agencies, for which specific purposes and whether there are any safeguards in place.

In October 2014, Information and Privacy Commissioners from every province and territory across Canada signed a joint statement calling for: an evidence-based approach to any proposed increase in powers; engagement of Canadians in an open dialogue on whether additional measures are required; and that any new powers come with enhanced oversight for intelligence and law enforcement agencies.

It appears that this discussion will now happen in Parliament. I hope there is a vigorous debate -- that tough questions are asked about the need and efficacy of these new powers.

Many voices – opposition parties, advocates, experts and commissioners are also calling for independent and robust oversight over our three national security agencies.

Commissioners will continue to advocate for transparency and independent oversight, and a mandatory review of this new law.

Privacy, Technology and the Future of Law

Biometric technologies, surveillance, and social media…. what do these three things tell us about the future of law?

First and foremost, they tell us that you will be practising law in an age of ubiquitous technology, where mass amounts of personal data are being digitized, shared, analyzed and monetized.

These tools have broad application and will transform the way you work, and the way we all think about information and data.

The technologies that will have the greatest impact on your generation probably haven't even been invented yet.

To those of you in this room who aspire to be the next generation of privacy law experts: we need you to bring your passion and sharp minds to the privacy challenges of today and tomorrow…. and be prepared to vigorously defend the enduring value of privacy in the digital age.

Last week the privacy commissioner of Canada released a public opinion survey that found 9 out of 10 Canadians are concerned about their privacy, with one third being extremely concerned.

Citizens care deeply about their privacy and will be looking to you to help protect it.

To those of you who will not specialize in privacy law… know that privacy issues will pervade your practice.

Privacy touches employment law, administrative law, human rights law, commercial and contract law and IP law.

Which is why it is important to be able to recognize privacy issues when they hit your in-box… and know how to address them when they do.

A few months ago I was on a discussion panel at a privacy and security conference. The moderator turned and asked me the following question:

"Is security still possible? Or is it more dead than that poor, ever-resurrected glittery zombie princess privacy?"

I responded by saying… not only is privacy still possible, it is, in fact, imperative.

Privacy is an enduring principle of great value to Canadians, one that underpins our collective right to freedom of association, freedom of speech, freedom of expression.

Despite statements to the contrary, privacy laws are in fact alive and well and are up to the challenge of the digital age.

Even after several decades of privacy law, the fundamental principles of notice, consent, openness, and use limitation 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.

This means that our laws are elastic enough to address the big challenges to privacy rights today... and those that have yet come in the 21st century.

I would like to close by referencing the best example of these principles in action I've seen in recent months.

It was the Supreme Court of Canada's decision in *R v. Spencer*.

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. The Court articulated 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.

Thank you for your attention and I welcome any questions you may have.