CHECK AGAINST DELIVERY

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

KEYNOTE ADDRESS TO THE

FREEDOM OF INFORMATION & PRIVACY ASSOCIATION INFO SUMMIT

SEPTEMBER 22, 2016

DREW MCARTHUR
ACTING INFORMATION AND PRIVACY COMMISSIONER FOR B.C.

Good afternoon and thank you for inviting me to speak with you.

I'd like to start by thanking Vince Gogolek and the FIPA board for the invitation. The Office of the Information and Privacy Commissioner has supported the Information Summit for many years and it's great to be here.

This is a new perspective for me. Thirty-five years of **being regulated**, and now I get to work for the other side!

As you know, former Commissioner Elizabeth Denham completed her term at the OIPC in early summer. She has now taken on the role of Information Commissioner for the U.K.

I've known Liz for **many years,** including through my involvement with the office's External Advisory Board, which she established to enhance the OIPC's research, public education, and policy work.

During her six years with the OIPC, Liz's accomplishments were numerous.

She brought about **real change** during her term and has left an incredible legacy. The U.K. is lucky to have her.

Fortunately, I don't have to fill her shoes for long because I can't walk in high heels!

I was sworn in as Acting Information and Privacy Commissioner on July 6. This is a temporary assignment.

According to FIPPA, a new commissioner must be appointed by a **unanimous recommendation by an all-party committee** within 20 sitting days, when the Legislature is in session again.

We expect this will be in the spring.

Kinda brings to mind the old Trooper song, for those of us who are old enough to remember it: "I'm here for a good time… not a long time…."

Some of you here may know me as "**the Privacy Guy**" from TELUS. I spent most of my career at TELUS and the former BC TEL, where we were subject to several different legislative regimes.

Now I have been given a unique opportunity to see privacy and access to information through the lens of a regulator.

And even though I will not be the permanent commissioner, I plan to use my time here productively. I want to build on the momentum this office has created, **especially** over the past two or three years.

I'm sure most of you are familiar with the office's **deleted email investigation**, *Access Denied*.

This report was important because it prompted the B.C. government to commit to passing duty-to-document legislation. They also committed to introducing penalties for those who attempt to deliberately destroy records… with the intention to frustrate the public's access to information rights.

Duty to document remains a topic of great interest not just here in B.C., but across Canada, as we heard just today in the session Vince moderated before lunch.

An important part of my job is to monitor government's commitments, and to comment, whenever necessary, as they continue to implement changes to records management and retention practices.

This office has **also monitored the implications** of new technologies, from automatic license plate recognition to employee monitoring spyware. And we will continue to do so over my term, beginning with **my first investigation report**.

But more on that later…

First, I'd like to share my perspective on what I believe are the qualities for an effective privacy commissioner:

to be a good **communicator**, to be an **advocate**, and to be a **leader**. Let me explain what I mean, and how I hope to demonstrate these qualities during my term.

Communication

I believe outreach and education are important responsibilities of my office.

We are developing a plan for outreach to communities around the province. We're hoping to reach key stakeholder groups, to inform them about the practical realities of privacy compliance.

This is the main reason I am here today: to enhance the public's awareness of what we're doing – and what remains to be done.

To that end, I'm hopeful I can convince you to **become ambassadors** in this respect… and in your day-to-day activities to **help me get the word** out about the important work of this office.

Advocacy

The second quality I'd like to touch on involves advocacy. Being an advocate for privacy does not mean lighting your hair on fire, although you can tell I'm not going to do that any time soon…

It means being **proactive**… taking the time to educate organizations and public bodies about how they can be privacy compliant while still balancing all of their other obligations.

Being an advocate also means providing guidance on emerging issues, as well as advice on more mundane operational issues.

I'll give you an example about how we advocated for **accountability**.

In the privacy world, accountability is about being legally responsible for processing personal data. It's also about building a culture of privacy within an organization.

Canada was the first jurisdiction in the world to write accountability into law in 2000. That's when the federal privacy legislation was passed… the *Personal Information Protection and Electronic Documents Act*, or PIPEDA.

But by 2010 it was obvious that many businesses did not understand accountability or how to implement it.

This is where **advocacy** came into play.

With our counterparts in Ottawa and Alberta, my office published a guidance document called “Getting Accountability Right with a Privacy Management Program.”

Why am I stressing this?

Because… my **first investigation report** as Acting Commissioner deals specifically with this topic.

My team looked at mobile device management within five B.C. government ministries – fitting, considering my background at TELUS.

I can’t reveal much more than that, since the report has yet to be released. But I **can** tell you that this investigation compared government’s privacy management policies and practices with the guidance document I just mentioned.

I hope that it will serve as an important learning opportunity for public bodies and organizations.

So watch for that report, coming out in the next few months.

Leadership

As Acting Commissioner, my goal is also to provide a supportive work environment... a place where employees feel valued, where they are given the appropriate tools and training to complete their work.

My years on the OIPC’s external advisory board helped familiarize me with the environment and strategic direction of this office. So, in my first few weeks, I was able to jump right into the job of leading the office through this time of transition.

I started by creating a plan for **my first 90 days** in the office. This plan dovetails with the office’s longer term strategy and identifies projects I’d like to accomplish during my term.

For example…

One task will be to manage and monitor the financial resources of the office. It sounds obvious, but we all must work within our budget.

Next, I’ll launch a **public awareness survey** that was initiated by my predecessor. This survey will help us tailor our public education efforts. The **outreach program** I mentioned earlier is an important part of these efforts, reinforcing our advocacy work.

My third task will be to address the backlog of complaints managed by the office. Liz spear-headed some great work in this area by implementing a continuous

improvement program last year. I want to build on those efforts by further reducing the backlog while still providing great service to our constituents.

The goal, in my mind, should be to spend **more** time being proactive and **less** time responding to complaints that come to us because organizations or public bodies are not be aware of their responsibilities.

I'm giving you these examples because even though the OIPC has a specific function – **to oversee and enforce B.C.'s privacy and access laws** – I must also be mindful about many other aspects of the organization. This includes the *Lobbyists Registration Act*, which my office also oversees.

So now you know a bit about where I come from and what I hope to accomplish during my term as Acting Commissioner.

Now I'd like to spend a few minutes highlighting some significant issues that we're watching here in our office....

Lawful Access

Lawful access has always been a challenging file for me, **especially** with my work in the telecom sector. Telecom companies have a significant amount of personal information about their customers… and are therefore **prime sources of evidence** during investigations by law enforcement agencies.

We've often seen… particularly on the federal level… that law enforcement continues to press for the use of new tools to conduct their investigations.

But I **strongly believe** that we must maintain the delicate balance between security and our fundamental right to privacy. Privacy is critical to personal freedom. And protecting privacy is also a **legal obligation** for governments and businesses.

Where there is a struggle between privacy and security, we need to carefully check the proportionality of the privacy intrusion against the demonstrated need.

When the balance is right – privacy and security **can** co-exist, building trust and confidence among citizens, stakeholders, and regulators. But when the balance is **not** right, trust is lost.

Law enforcement, while certainly a challenging field of work, is staffed by people like you and me who are looking for the most expedient way of gathering information. Their focus is on public safety, where **more** information is generally better.

Given a tool for one purpose, we can often see **another use** for the same tool. Where it gets tricky is that the other use **might** not be authorized.

Let me give you an example from when I was “privacy guy” at TELUS. Some years ago telecom companies across Canada collaborated to provide law enforcement agencies with a tool for investigating one type of serious crime – child exploitation.

We felt, given the egregious nature of the crime, that it was **important** for us to assist law enforcement. And PIPEDA allowed for that.

This tool was designed to give them basic information: customer names and addresses when they provided a cell phone or IP web address associated with child exploitation.

When used for legitimate purposes, there was no issue. But it is **perhaps not surprising** that law enforcement might try to use that tool for other investigations.

I remember back in 2005, when Jennifer Stoddart, Canada’s then-privacy commissioner, was the victim of social engineering or pretexting initiated by a reporter. Data brokers from the US were able to unlawfully convince customer service representatives to provide information on her telephone bills.

But it turned out that some of the regular users of those data broker services in the US were law enforcement agencies!

Bill C-51

Let me turn to the national security legislation passed last fall by the former Conservative government following the attacks in Ottawa and Quebec. Bill C-51 provides broad new powers for CSIS, CSE, and law enforcement agencies in Canada and elsewhere.

We all know that security is essential to maintaining our democratic rights. But I’m **not convinced** that these measures were designed in a way that protects freedom of speech and the privacy rights of individuals. And that delicate balance between security and privacy.

With the recent change in the federal government, the future of that Bill remains uncertain, as officials consult with security experts, civil rights advocates, and the public on how to structure the country’s security framework. We will be watching for the outcome of this consultation.

I have some concerns regarding the recent **online public consultation** from the Public Safety minister. In my opinion, this discussion paper paints a biased picture of the need for security… because it doesn’t emphasize the rights of the individual while describing the challenges faced by Canada’s security establishment.

Whatever the result of these consultations, **we must ensure** that the tools we give law enforcement are appropriate and that there is oversight of the investigative processes.

The Future of FOI and Privacy Law

When it comes to what the future holds for FOI and Privacy Law in B.C., I wish I could be clairvoyant, like Johnny Carson's Carnac the Magnificent.

We've made our views known through **two** recent legislative reviews – PIPA in 2014, and FIPPA this past spring. Two Special Committees listened carefully to our recommendations before producing their reports.

I've already mentioned the government's response to the duty to document recommendation. Now I'd like to tell you about some of the other recommendations we made recently to the FIPPA committee… recommendations that I'm pleased to say **were accepted** in their final report.

The first was that the law be amended to require public bodies to implement privacy management programs. These programs would be **sensible** - tailored to the structure, scale, volume, and sensitivity of an organization's operations. But they would, in a very real way, assist public bodies in meeting their legal obligations under FIPPA.

The Committee **also** recommended mandatory notification of privacy breaches, a key element of effective privacy management.

Mandatory breach notification is important because it would alert my office to any potential harm that could result when personal information is breached.

It would also provide my office with the opportunity to help mitigate the harm that could come to individuals who are affected by a breach.

We were also pleased that the committee recommended increased penalties for the unauthorized destruction of records and inappropriate disclosures of personal information. Increasing penalties for **all privacy offences** – not just "snooping" incidents – would help assure the public that their privacy and access rights are taken seriously by all public bodies.

We'll continue to talk with government and keep these issues front and centre. Meanwhile, we're also watching Europe, as the European Union prepares for the 2018 roll-out of the General Data Protection Regulation.

That regulation applies to **any** organization that holds EU citizen data. And it carries strict requirements and significant administrative monetary penalties for non-compliance – up to 4% of a company's global revenue. That's **significant**.

Regardless of the outcome of these and other legislative processes, we can all agree that access to information and privacy concerns touch many aspects of our public and work lives. And the scope of the work we do seems to expand, each and every day.

I've talked a bit about the current environment we find ourselves in and how we got here. I would now like to talk briefly about the **future of privacy**. My successor will definitely face some challenges!

Today, data can travel almost as fast as the speed of light. And it knows no borders. That's why this office works closely with international groups of privacy regulators, including the Global Privacy Enforcement Network and the Asia-Pacific Privacy Authorities or APPA. In fact, this summer my office assumed the role of secretariat for APPA.

My Office is also a partner in a Big Data Surveillance Study with four universities across Canada. With these efforts, we are learning, participating in information sharing, and taking on a leadership role.

The conversations about big data will remain top of mind with this office long after my term comes to a close.

The Internet of Things will continue to expand, as **more and more** smart devices and appliances are invited into our homes and lives, sometimes with significant privacy impacts.

Did you know that by interpreting wifi signals – that's radio waves, not the content – it can be determined if you are lying down or moving about within your wifi area?

Connected cars are another area of potential concern. Just think of it – in the future, with the myriad of real time sensors being added to driverless cars, your car could provide **historic** and **real-time** geo-location data of your every move… with commercially valuable applications.

Concerning, isn't it? The truth is that in our world, we never **really** know what's just around the corner. It could even be an Amazon drone, out on a delivery call.

That's both exciting **and** challenging, at the same time.

But one's things certain… looking through the lens of a regulator these last few months has **really** broadened my understanding of our common challenges and goals.

Thank you again for inviting me here to speak with you today.

Please remember, my office is always open for consultation.

Let's work together to develop solutions in today's complex privacy environment.