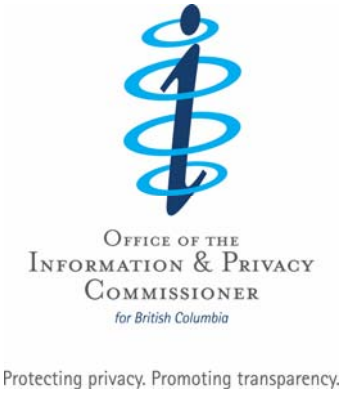

CHECK AGAINST DELIVERY

PRESENTATION TO THE 18TH ANNUAL PRIVACY AND SECURITY CONFERENCE

FROM REGULATED TO REGULATOR: TWO PERSPECTIVES ON PRIVACY

FEBRUARY 9, 2017

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

Introduction

Good morning and thank you, Colin for that kind introduction. Much like you, and many of our audience members and other speakers, I have a long history with this conference.

Colin, it's good to see you here today as Master of Ceremonies. I have attended many times over the years, sometimes as a guest, sometimes as a guest speaker often as a panel member. And last year, I was the MC. You certainly have big shoes to fill!

I have been looking forward to this year's conference as it will be my first (and potentially only!) time I'll be able to speak to you as the Acting Information and Privacy Commissioner for B.C.

A permanent commissioner must be selected based on a unanimous recommendation from an all-party committee. This will possibly happen with the

legislature sits again… and no, I don't have any special insight into who the next Commissioner will be!

The best minds in privacy and security are here at this conference, sharing ideas and learning new things. Though we may not always agree, we have a common goal: solving the privacy and security issues we face, each and every day.

Role as Acting Commissioner

Around this time last year, I was semi-retired, spending as much time as I could on my boat, or playing golf or hockey. When I wasn't pursuing my favourite sports, I spent my time working with the OIPC's External Advisory Board, chairing the national board of the Arthritis Society, and running a small consulting company.

I could never have guessed that I would be here today as the Commissioner!

I spent most of my career at TELUS and the former BC TEL. Now I'm responsible for enforcing B.C.'s privacy and access to information legislation. So I've gone from being regulated to being the regulator… and it's been quite an eye opener for me.

From Regulated to Regulator

I'm often asked if I see the world of privacy differently now that I am in the role of regulator. It reminds me of the time when I was the Chief Privacy Officer for TELUS and attending a conference where Colin Bennett was giving a presentation after writing one of his many books on privacy. Colin asked the audience "who here thinks they are a privacy advocate?"

Of course I put up my hand. He seemed a little -- how shall I put it – sceptical?

But really, a Chief Privacy Officer is a privacy advocate within their own organization, and they often deal with formidable issues. Just consider the volume of information a telecom company collects.

Many years ago, the amount of data we collected was so large that, using our mainframe computing power of the day, we had to run our billing cycle in four phases each month. Add to that, text messages, voicemails, emails, web browsing history, even third party information. There's a lot of information being collected, about all of us.

As a privacy advocate, I had to ensure that we limited collection of personal information, that we protected what we did collect, and that we trained literally thousands of employees. All that while working under a number of federal and provincial privacy regimes.

See Colin, I was a privacy advocate. So, to answer the question about whether I've changed my perspective on privacy now that I'm the Acting Privacy Commissioner, the answer is: "Yes".

When I was at TELUS, my view into the world of the privacy regulator was not clear, kind of like looking through the wrong end of a telescope. I had a very good understanding of how privacy legislation affected me, my business, and my industry… but that was all. I couldn't really see what was going on on the other end

When former Information and Privacy Commissioner Liz Denham asked me to join the office's External Advisory Board in 2010, my view of the office and privacy regulators came into clearer focus. Over the past six years, I began to better understand the challenges regulators face, the scope of work they take on, and how mindful they must be of the interests between parties when considering privacy and access to information issues.

Now that I am privileged to see this office's activities through the lens of Acting Commissioner, my focus has sharpened significantly. I've watched staff view every new technology or privacy threat not only with a telescope, but with a microscope. The behind-the-scenes work of my team is absolutely amazing.

When I was viewing the regulator from a distance, I was curious about how complaints were reviewed and processed. Now that I've seen the inner workings of the OIPC, I must say that the operations of this office are much more complex than I ever expected – and much more thorough.

I am impressed with the administrative justice and the amount of precedent-setting work that goes on here. While not all of it is earth shattering, it speaks to the thoroughness of the staff and their commitment to ensuring that we get it as right as possible at the outset.

While the Acts that we enforce provide us direction and guidance, we often have to consider other factors such as existing jurisprudence from previous decisions, court cases, and rulings in other jurisdictions. My staff takes considerable care to ensure a careful balancing of interests in the cases we address.

When I worked at TELUS as Chief Privacy Officer, I can remember feeling resistant to the idea of regulation. Like most individuals, I didn't think I needed a law to make me do the right thing. I remember feeling frustrated when I would get a letter of complaint from the federal privacy commissioner, and also feeling at the time that they just didn't understand the complexity of our business.

But over time, I began to see the broader impact of privacy regulation, that it was much larger than me, and my team, and even my business. I came to see that privacy regulation holds everyone to a higher standard than they may hold themselves. And in the telecom industry, this was important – because even though in my opinion TELUS standards were very high – not all Telco's are created equal. I

believe it instils customer confidence in the entire industry if a minimum standard is achieved.

What I see differently now

Now I'd like to touch on some things I see differently after sitting in the regulator's chair. One area I have a clearer understanding of now is solicitor-client privilege. In my previous life, I had maintained that privacy commissioners should not be the ones to determine whether or not something should be withheld from disclosure because of solicitor-client privilege.

Well, as an independent, quasi-judicial body, I've learned that we need to have all the information in front of us so we can determine if in fact solicitor-client privilege applies.

We cannot do that if we don't have all the relevant information.

When we can review privileged documents we are better able to mediate complaints, AND, I now realize, we don't prejudice one party over the other in the outcome. This is beneficial to the parties involved because it avoids the often costly and time-consuming court process. Resolving these questions through an administrative tribunal such as my office, rather than through the already over-burdened court system serves an important public good.

The recent Supreme Court decision regarding the University of Calgary has not changed our approach in this area, as BC's FIPPA differs significantly from Alberta's. Our Act specifically references solicitor-client privilege, while Alberta's Act does not – and this difference is noted by the Court in its decision.

Another area I see differently now is mandatory breach notification. When I was at TELUS, we spent a great deal of time working with other Telco's across the country as well as the federal and provincial commissioners to put together voluntary breach reporting guidelines. I can say one of the reasons we did so was to avoid having it thrust upon us as legislation. Well, that ship has long since sailed, especially given the new GDPR regulations, oh, and perhaps the continuing proliferation of breaches.

It makes sense to have privacy commissioners as the monitors and examiners of breach circumstances to help organizations mitigate the risks associated with privacy breaches. Most forward-thinking organizations now look at it as breach readiness, not just breach response. And they test their breach readiness just like they would their emergency response plans.

We all know privacy breaches carry a significant cost. They put individuals at risk for identity theft and can cause serious financial or reputational harms. Breach reporting in BC is currently voluntary in both the private and public sector, although my office has recommended that it be made mandatory for both.

National security

As you've heard, I have changed my perspective, and therefore my position on a number of significant issues.

But one area where my views haven't changed, in fact, where they have been reinforced since becoming Acting Privacy Commissioner, is national security.

We've all heard the saying, "You can have security without privacy, but you can't have privacy without security." That said, there are times when security challenges our rights to privacy, and I see it as our role as commissioners to ensure that we take on these issues, whether they are the security establishment going beyond the rule of the law or organizations taking their security processes beyond what is reasonable in the circumstances.

Earlier this morning we heard Stewart Baker say that privacy laws are the result of technological panic. It won't surprise you to hear that I disagree.

During my time at TELUS, the federal government tried to increase the powers of law enforcement agencies to collect information. They recommended that telecom service providers store information on every call, text message and email, in case a production order might be issued.

We see this still going on; in fact, with calls from many governments to have increased retention and access to phone and internet records. Witness the UK passing legislation requiring the retention of ALL information by telecom carriers for periods longer than would otherwise be required for their business needs.

I have two main concerns about the increasing demands by governments to mandate the retention of otherwise unnecessary information: the unintended consequences of over-collection of personal information; and the potential misuse of that personal information, whether by government or private businesses.

We've seen many scenarios that give us pause, such as when law enforcement spied on the cell phone use of a number of journalists to track their location and, in one instance, to identify a confidential source. This journalist was not the subject of the investigation, but instead was spied on because he had contact with a subject. In my view this surveillance should have us all worried, as it's likely that many more instances like this occur and are unchallenged.

I'm not looking to sacrifice security for privacy. I don't believe it's an either/or scenario and I don't think it benefits anyone to view it that way. We all know that security is essential to maintaining our democratic rights, as we have seen serious and tragic events occur on our soil. But I strongly believe that if we lose our privacy in the process, we lose our democracy as well.

Recently, I was honoured to join Canada's privacy commissioners and provide a unified stance on our national security framework. Jointly we provided a submission in response to Public Safety Minister Ralph Goodale's green paper, emphasizing, among other things, that we need proper oversight of the surveillance activities of national security and law enforcement agencies.

The security imperative, either at the national or local level, must still allow debate about privacy rights and obligations. Police and privacy commissioners need to respect one another's mandates. The public expects us to work constructively through these issues as they arise, and so we must.

Work completed while in the office

I would like to turn now to some of the valuable work has been done within the office in the past eight months.

When I first took on the role of Acting Commissioner, I put together a 90-day plan to set my immediate priorities. One of these line items was eliminating our backlog of outstanding investigation files—a situation that I suspect many of you may have been familiar with. This is a task that had been embarked upon by my predecessor as part of a continuous improvement process. I'm proud to say that through the team's various initiatives, the office's backlog of files has now decreased from 290 a year ago to 27 today.

This past October, together with the BC Auditor General, we released an investigation report into mobile device management by the B.C. government that made several recommendations for improvement and included a useful guidance document, published on our website, for both organizations and individuals.

And, in December, we released the results of our first-ever audit of a private sector business in B.C.: a clinic in the lower mainland that had installed eight video surveillance cameras throughout its premises. My audit concluded that this surveillance was unlawful. We used this audit as an important opportunity for public education, and a reminder to private businesses that they should only use video surveillance as a last resort after exploring other less privacy-invasive options.

I have a strong position on video surveillance. Perhaps my perspective is influenced more by the proliferation of cameras than anything else. At TELUS there were many instances where folks wanted to install video cameras that were inappropriate. I can say there were quite a few that were appropriate as well, but the threshold seems to have lowered over the years with the mass availability of surveillance cameras. In some circumstances, video surveillance is justified, but in other instances, such as in the case of this clinic it is invasive and excessive.

This leads me to what's coming next for the office – which is an audit of ICBC's information sharing agreements. ICBC collects a vast amount of information about the majority of BC residents. Think about it – to become insured and operate a motor

vehicle, you have no choice but to hand over your personal information. Many other organizations are given access to this information, such as Translink to charge bridge tolls or parking lot operators to issue tickets.

Our audit will determine what information-sharing is taking place, whether it is lawful, and whether the security of our personal information is adequate. I may not be in office for the results of this report, but the work is now underway.

Collaborative work

In addition to the work we do in B.C., our office is an active member of two international associations of privacy regulators: The Global Privacy Enforcement Network, or GPEN, and the Asia Pacific Privacy Authorities (APPA). For the past six months, my office has served in a leadership role as secretariat for APPA.

Why do these interactions matter? Well, for one, the experiences shared in these information networks can offer great insights for member regulators. Sharing as a group gives us advance warning about emerging challenges and technologies.

We also get to problem-solve together. We promote privacy rights together. And we investigate together, like the recent work of the Privacy Commissioner of Canada, the Australian Information Commissioner's office, and the US Federal Trade Commission with their joint investigation of the famous Ashley Madison breach. We weren't the lead on that investigation, but our office was consulted in the process.

Conclusion

But what I'm most proud of – continuing the work of previous commissioners, is how this office makes a difference to the citizens of B.C.

I've seen how other provinces and other countries view this office as a leader. I've seen how the office is a bit of a trailblazer, looking ahead at privacy and access issues. And I've seen how this office deals with emerging issues – such as big data and ethics.

I'm very proud of my staff. I get to work with an amazing group of people. And I think that the public bodies and organizations in general have welcomed me to this role, and I've really enjoyed getting out and talking to groups across this province. So I thank you for that opportunity.

Soon – probably within weeks, the legislative committee will release its decision about the next permanent commissioner. I love this job, and if it wasn't for the fact that I love retirement more, I would have seriously considered applying for the position.

It's been a remarkable experience and a great privilege to hold this office. Thank you for your attention this morning.