Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

PRESENTATION TO

THOMPSON RIVERS UNIVERSITY 4TH ANNUAL PRIVACY AND SECURITY CONFERENCE

JANUARY 31, 2018

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

Good morning and thank you Alan for your introduction. I'd also like to thank Laurel Wale for the invitation to spend some time on your beautiful campus. It's great to be here at Thompson Rivers University as part of your conference for Data Privacy Day.

Over the next 30 minutes, I'll share my perspectives on how to best protect personal information from cyber criminals. I'll attempt to demystify de-identification. I'll fill you in on the provincial government's new Data Innovation Program - and why it gets more than a passing grade from my office when it comes to data protection. And I'll tell you about some recent work of my office.

But first, I would like to start off by giving you a brief overview of my role at the Office of the Information and Privacy Commissioner.

I was appointed to this role in June 2016, and will hold the position until a permanent Commissioner is chosen – unanimously, I might add - by a Special Committee of the Legislature. I expect this will be in the near future.

As Acting Information and Privacy Commissioner, I am responsible for enforcing the *Freedom of Information and Protection of Privacy Act,* or FIPPA, which applies to 2,900 public bodies in BC, including government ministries.

I also enforce the *Personal Information Protection Act*, or PIPA, which applies to over 380,000 private sector "organizations" including businesses, charities, associations, trade unions, trusts, and even political parties, which I'll discuss in more detail later.

In addition, as Registrar of Lobbyists for BC, I also am responsible for enforcing the *Lobbyists Registration Act*.

My office investigates, mediates, and resolves appeals regarding access to information disputes. We also investigate and resolve privacy complaints, and we issue legally binding orders. We also comment on the privacy implications of new technologies and/or data matching schemes, assist with privacy impact assessments, and educate and inform the public about their access and privacy rights.

Now let's move to the pressing issue of cybersecurity.

I think we can all agree that data breaches are becoming far too common. And the size of these breaches is **staggering**. Consider the most recent Yahoo breach announcement. This incident, dating back to 2013, has the dubious distinction of being the biggest data breach in history.

One billion email accounts were compromised. **One billion.**

Around the world and across the street, our personal information has never been more at risk. And the cost of cybercrime is also increasing – last week's World Economic Forum stressed the accelerating risks and costs of cybersecurity.

Experts estimate that the aggregate economic cost of cybercrime is now more than $1tn US per year – and expect that figure to grow to around $8tn over the next five years.

Now **there's** a growth business, if I ever saw one.

While these numbers are difficult to comprehend, they definitely highlight the severity of the problem.

Why has cybercrime increased at such a rapid rate? Data centralization is one key factor. And as data becomes more mobile, it's much more easily accessed.

Another reason is "shareability." Data can flow between organizations and around the world in seconds with just a single keystroke.

And how data is being sliced and diced today is another concern of my office. At our own BC Aware event this past Monday, Eric White from Victoria's Myra Systems

gave a riveting session about how machine based learning is growing exponentially across many, many industries.

Artificial intelligence is also burgeoning in the public sector. For example, I learned recently from one of BC's health authorities about an AI tool they are using to adapt medical forms to improve them "automatically."

Then there's our connectivity to the Internet of Things – or the Internet of Everything, as I like to say. This is yet another risk factor. From baby monitors to smart refrigerators, our personal information is under constant threat.

How many of you have Alexa installed in your home? Or Google Home?

These devices are smart, and they're certainly convenient…

For example, I can open my front door in Port Coquitlam with my phone.

But **convenience** at **what cost** to our privacy?

And of course…. There's also video surveillance. Today's inexpensive, easy-to-install surveillance systems surround us 24/7, and in my opinion, are contributing to the over-collection of personal information on the street, in parks and neighbourhoods…. even in the workplace.

Think about the new cashier-less AmazonGo store, now open in Seattle. No lines, no checkout – just grab and go, says Amazon.

It would be convenient. But again, at what cost?

How would **you** feel about hundreds of cameras watching – and analyzing – your every move as you're shopping?
Are you comfortable with that?

One thing I know for sure is that gatekeepers of data have increased challenges… and with innovation comes additional responsibilities.

Let's look at a few specific examples that have affected Canadians…

Bell
Last week telecommunication giant Bell alerted its customers after hackers accessed the personal information of, they said, "fewer than 100,000 customers." Fewer was **their** emphasis – not mine. Names and email addresses were illegally accessed and, in some cases, phone numbers and user names. Credit cards were "not thought" to be affected. Again, their emphasis, not mine. Incredible, isn't it, how 100,000 people is thought to be a small breach these days.

Ashley Madison
The Ashley Madison breach was sensational, and I don't mean in a good way. This breach impacted more than 40 million people, and exposed very sensitive information held by the online dating site.

This is a good example of why it is so important to think about the type of information you are putting online. If you are concerned about maintaining anonymity in the event of a hack, consider whether your email, username or geo-location would give away your identity. It's this centralization of data that increases the risk to individuals.

This is also a learning opportunity for other organizations, as the fallout of this particular hack has included alleged blackmailing and public shaming of Ashley Madison's clients.

My office worked with the Privacy Commissioner of Canada, the Australian Information Commissioner's office, and the US Federal Trade Commission on this case.

This example illustrates the challenges we regulators face in trying to battle cybercrime.

Now I'd like to share a few examples of privacy breaches a little closer to home.

Ministry of Education Breach
The first involves a missing portable hard drive. In September 2015, the Ministry of Education notified the Commissioner that it was unable to locate a device containing the personal information of **3.4 million BC students and teachers and Yukon students**, collected between 1986 and 2009. In her investigation, my predecessor found that the Ministry failed to provide adequate security for this information.

One of the most frustrating findings in this case was that if ministry employees had complied with **any one of their own existing policies and directives**, the hard drive would not have been lost in the first place.

So what are the takeaways for other government departments and organizations?

Well, first we need to shift our views about personal information.

Personal information is more than numbers and names. It's an **asset… a powerful, digital currency that trades on world markets.** Governments and organizations should treat personal information with the same level of security and care they provide for financial assets. Losing personal information is a much greater liability that losing cash.

Imagine if we treated personal information as if it was cash – we'd know where it was at all times. It begs the question: why do we have more controls over cash than we do over personal information?

Another important message is that policy alone is not enough to prevent a privacy breach. Policy is just the paperwork of privacy.

While strong privacy and security policies are essential, ensuring compliance by employees – building in checks and balances - is the real ground work of privacy management. I'll get into more about this in a few minutes.

Video Surveillance – Medical clinic
But first, another BC example – this time, involving the over-collection of personal information through video surveillance. A medical clinic in the lower mainland had installed eight video surveillance cameras throughout its building – including the lobby, fitness rooms, and hallways. My audit concluded that this surveillance was unlawful. We used this report as an opportunity for public education and as a reminder to private businesses that they should only use video surveillance as a last resort after exploring other less privacy-invasive options.

Saanich
The students I met in Assistant Professor Ryan Gauthier's law class yesterday were particularly interested in this next example.

In 2014, the District of Saanich had a security issue. So they decided to install software called Spectre 360 to deal with it. Unfortunately not all solutions can be pulled out of a box.

By installing this software, they enabled all sorts of features they didn't need to fix their security problems… features like keystroke logging, automated screen shots, and continuous tracking of computer program activity.

An employee's every keystroke and email, or screen captures of computing activities at 30-second intervals, clearly exceeded what was authorized under our privacy law.

In our investigation, we found that the District could only collect personal information that was directly related to and necessary for the protection of its IT systems and infrastructure.

We made five recommendations on that investigation, most importantly the implementation of a comprehensive **privacy management program.**

Privacy management programs
What is a privacy management program? It's a proactive plan for protecting personal information.

Privacy management programs work because they are scalable for organizations of all sizes.

My office published a guidance document called *Getting Accountability Right with a Privacy Management Program* as a **blueprint** for organizations who are committed to

protecting personal information. The document is available on our website, www.oipc.bc.ca.

One of the first steps is to appoint a Chief Privacy lead – someone who is responsible for privacy in your organization. This person should have a voice at the executive table and should be empowered to lead the privacy agenda. This incidentally was a role that I was asked to take on 17 years ago with TELUS.

Next, program controls are identified, followed by ongoing assessment and revision––this step is critical in light of changing threats and risks.

Let me underscore the word "**ongoing**."

Privacy and data protection is not a "once and done" activity. Rather privacy management is best included as part of a broader risk management program.

Coming in 2018 – we will be offering the private sector a self-assessment tool…. Stay tuned for more information on that.

Data Innovation program
I'd like to give you an example of a research project that takes the right approach…. Last year, we were asked by the BC provincial government to review their new Data Innovation Program.

This initiative, which will soon be implemented, is designed to provide a secure environment for data scientists, analysts and researchers in government and academia to access and generate insights from high value de-identified data from across the public sector.

The key word here? **"Deidentified."**

De-identification is the process used to prevent personal information from being connected to an individual's identity. It's a very effective tool in the protection of personal information. But it doesn't stop there.

Research and analysis in the Data Innovation Program will only use **linked, de-identified** data in a **highly secure** research environment.

And there will be other safeguards, too: **only anonymized, non-personal information will ever leave the centre's secure environment. This** program is about **population-level research and analysis, never individual-level decisions**. It can't be used to track or monitor or make any decisions about individuals, but does enable research.

This is a **great** example of built-in **privacy**: both privacy **and** security have been considered at **all** stages of the program's design and build….

For instance, even though the data is de-identified it is still protected as though it is personal information. This is a critical safeguard. Yet the program's privacy and security measures will not compromise the efforts of researchers.

The program builds on the efforts of Population Data BC, or POPData, who work with the Ministry of Health to provide privacy protective access to academic researchers.

My Office was consulted on the program's Privacy Impact Assessment or PIA. For those of you who are unfamiliar with PIAs – they are important tools that help to identify and address potential privacy risks before programs are up and running.

The Data Innovation Program will ensure compliance through third party certification and that a Chief Privacy and Security Officer will be appointed. This individual will be responsible for ensuring that best practices are continuously followed.

These are precedent setting examples on how we can properly conduct research in a privacy sensitive way.

Other measures to protect PI

As consumers, we need to remember that we have responsibilities too when it comes to data protection.

Take multi-factor authentication. Most email providers offer it – we just have to care enough about our data privacy to use it. Just last week, a Google engineer said that less than 10 percent of all active Google account have adopted this extra security step.

A study out of Singapore last fall indicates that hackers could use smartphone sensors to crack 4-digit user PIN codes – the researchers had a 99.5% accuracy rate when they tried to hack phones that had one of the 50 most common PIN codes.

Why not take the extra step to secure your devices – with a thumbprint, for instance?

Then there's **encryption**. It works! Just ask the FBI. They continue to complain that they cannot gain access to encrypted wireless devices.

It is an easy way to secure digital information. It is the standard when storing personal information on a laptop or any mobile storage device. And did I already say it is easy?

A word of warning, though: today's encryption standards may not meet the test of tomorrow. That's why ongoing risk management, as I mentioned earlier, is so important.

My office has seen too many of these breaches over the years – not just this Ministry of Education example - that would have been prevented had encryption been

enabled. It is a minimum standard to safeguard personal information that is often overlooked.

What are we working on now?
We are currently investigating the over-collection of personal information by landlords receiving several complaints every week from potential renters. This is an important investigation, as individuals may be reluctant to assert their privacy rights at the risk of losing housing options. Just imagine being asked for your children's report cards when applying to rent a home.

We are also investigating the collection, use and disclosure of personal information by political parties. I am looking into whether the BC Liberal, New Democrat and Green parties are in compliance with PIPA based on the vast amounts of personal information each party receives during the election process. My office has received numerous complaints about this issue, along with reports of privacy breaches by these parties.

Conclusion
I hope my remarks today have expanded on some of the complex challenges we all face as we grapple with our brave new digital world. These challenges are exactly why we collaborate with colleagues around the world to ensure British Columbia's data is properly protected.

We are carefully watching Europe's upcoming implementation of the General Data Protection Regulation (or GDPR) with particular interest. By May 2018, businesses AND public bodies that process personal information of EU citizens will have to adjust their privacy practices or face some pretty severe consequences.

For serious contraventions – 20 million Euros, or 4% of annual worldwide turnover of the corporate group, **whichever is higher.**

For lesser contraventions – 10 million Euros, or 2% of annual worldwide turnover of the corporate group, **whichever is higher.**

These are significant fines.

The GDPR is all about accountability – and it will be a real game changer for all jurisdictions in terms of global privacy principles.

BC will need to react, and it is our hope that some of our recommendations for improvements to FIPPA and PIPA will be implemented in the coming months.

Thank you again for welcoming me here to mark Data Privacy Day with you. Working together, we are better poised to take the challenge of protecting personal information. I look forward to continuing this conversation with you throughout the day and beyond. I welcome your questions now, if we have time.