Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

**CHECK AGAINST DELIVERY**

# KEYNOTE ADDRESS TO THE

# FREEDOM OF INFORMATION & PRIVACY ASSOCIATION INFO SUMMIT

## SEPTEMBER 21, 2017

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

Good morning and thank you Vince and the FIPA board for inviting me to speak today.

You know, last year I joked that I was "here for a good time… not a long time…"

But as it turns out, that's not quite true!

As most of you know, my term was extended when the legislative committee tasked with selecting a permanent Commissioner was unable to reach a unanimous decision – after two competitions and meeting 19 times!. Now the house is sitting again, and a committee is yet to be appointed, but I've been assured that my expiration date of October 25 will be addressed.

So, I've been here for a good time… AND a long time. It's been a privilege – and a learning opportunity.

Today, I'd like to talk to you about some of the work of my office over the 15 months – beginning with our most recent reports.

We've been pretty busy: we published an audit of mobile device use in the BC government, conducted our first private sector audit, and examined ICBC's information sharing agreements.

But I'd first like to tell you about our most recent report, which we released just yesterday.

**Reports: Timeliness**

This special report will no doubt interest everyone in this room – especially with Right to Know Week just around the corner. It also speaks directly to my mandate: which is to enforce compliance with the Freedom of Information and Protection of Privacy Act.

*Timing is Everything: Report Card on Government's Access to Information Responses* is the name of our report and it examines the timeliness of government ministries in responding to FOI requests.

We compared and analyzed the results with previous timeliness reports of this office, from the most recent report in 2014 dating back to our very first timeliness report which was published in 2009.

The results are… how shall I put it? Not very encouraging.

In fact, I am pretty disappointed.

As most of you know, public bodies are required to respond to a request for records within 30 business days. Time extensions are permitted, but only under specific circumstances:

- when a public body needs more detail about a request,
- if a large number of records are requested or must be searched,
- if more time is needed to consult with a third party or other public body,
- or if the applicant has consented to the extension.

When we reviewed government's compliance with FIPPA in responding to access requests, we found that from 2013-2017, it was in contravention of the Act between 20 and 26% of the time. Just think about that. In other words, in some years, one in every four access requests was not responded to within the timelines required by FIPPA.

Previous timeliness reports from my office also confirm that government routinely operates in contravention of FIPPA.

This should be an extraordinary finding.

But somehow… non-compliance with FIPPA has become normal for government.

When I was chief compliance officer at TELUS, my job was to ensure the company complied with the various pieces of legislation we were subject to. Eighty percent would not have been good enough.

So my first and most important recommendation in this report is that government **must** take whatever action necessary to come into compliance with the law.

I am also very concerned with the **significant** increase in government's time extension requests to my office over the past two years. The lack of compliance with FIPPA has occurred even though government's use of time extensions has steadily increased since 2008.

My office plans to follow up with another timeliness report for this current fiscal year. I hope government brings itself into compliance with the law by the time we release that report.

Okay.

My blood pressure is starting to return to normal.

**Other reports**

We released another report last week that was a little less stressful for me: an audit of ICBC's Information Sharing Agreements.
Why pick on ICBC? Well, for the simple reason that it holds one of BC's most complete personal information data-sets – just think about it. They have personal information of virtually every adult in BC.

Driving information, vehicle ownership information, insurance information. Contact info. Physical description including your photograph, height, weight, eye colour, hair colour. Plus driving history, infractions, and insurance claims.

There's quite a lot of information there, and if it got into the wrong hands, it could have serious consequences for individuals.

And ICBC shares that information with many other organizations, from bailiff services and municipalities to parking lot operators and tow companies.

For the most part – I'm happy to report – ICBC is fulfilling its duty under FIPPA to protect the personal information of British Columbians. There were some areas of ***potential*** risk – which ICBC says they will immediately address.

We're also investigating TransLink, in light of reports that the transportation authority shares Compass Card information with law enforcement agencies. Stay tuned for the results of that investigation.

Working backwards in time now – stay with me – we released the results of our first-ever audit of a private sector business in BC last December. 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 important 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.

And shortly after I spoke to you last year, we published an investigation into mobile device management by the BC government. Working together with the BC Auditor General's office, who also released a report, we published a useful guidance document about mobile device security on our website for both organizations and individuals. I encourage you to check out that guidance available on our website to ensure you take the basic steps to protecting your use of mobile devices.

**Surrey Creep Catcher**

Another issue we have been dealing with involves a citizen vigilante organization known as Surrey Creep Catcher.

Here's what happened: Two individuals complained to my office that Creep Catcher had improperly collected, used and disclosed their personal information. The organization had induced each individual to have online communications with a fictitious woman over the age of 18. Then they told the individuals that this decoy was under the age of 16 and arranged a meeting to confront each man for attempting to lure a minor. The organization recorded the encounter and uploaded the video to Facebook and YouTube.

I found that Surrey Creep Catcher's conduct violated PIPA and ordered them to stop collecting, using and disclosing the complainants' personal information, to destroy all of their personal information in its custody or under its control, and to ask others who disseminated the information to remove and destroy it as well.

Well Creep Catcher has petitioned the BC Supreme Court for judicial review.

We're currently preparing a response, but in the meantime my order is stayed.

A few things are unique about this situation – I can't recall another time where an organization has publicly defied a commissioner. It may be the first time EVER that a privacy commissioner has been called an idiot in the press. Normally that comment is reserved for my immediate family and friends. Perhaps a few colleagues. But I digress.

**Fowl Surveillance**

Oh, and there's another catching organization I am investigating – a chicken catching organization that ran afoul of the law.

You might remember an incident reported in the media where chickens were being mistreated on some BC farms. The organization responded by implementing body-cams on their supervisors to record video and audio of company employees.

This was reported in the media, which immediately got my attention. As I've noted in the past, there are very few times where continuous video surveillance of employees would be authorized by BC's privacy laws.

This investigation report will be published soon and will provide some important considerations for any organization considering implementing video surveillance.

**Leadership and corporate initiatives**

Turning briefly to work within the office now.

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 as Acting Commissioner, I was able to jump right into the job.

First thing I did was create a plan for **my first 90 days** in the office. This plan identified projects I wanted to accomplish during my term. One of these projects was to launch a public awareness survey – an idea initiated by my predecessor Liz Denham – to help us understand how knowledgeable average citizens are about BC's privacy and access to information laws and their rights under those laws.

These and other questions formed the basis of a comprehensive BC Stats resident survey, the first of its kind ever conducted by the OIPC.

We learned a lot from the survey.

For instance, we learned that just under half of BC residents (46%) are familiar with BC's access to information and privacy laws – **and only 3%** consider themselves to be very familiar with these laws.

That must be pretty much all of you here in this room!

We also learned that while half of BC residents surveyed had heard of the OIPC, 68% wish they were more informed about the Commissioner's Office. These answers will help guide our future outreach efforts.

We also recently completed an update of our Strategic Plan, with critical input from staff and our external advisory board. We'll be publishing the plan on our website soon, so watch for that as well.

## Collaboration

In other areas, my office continued to work closely with our federal and provincial counterparts over the past year. 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.

I believe that police and privacy commissioners need to respect one another's mandates and am closely following the debate on Minister Goodale's bid to increase the abilities of Canada's border services to collect exit data, which got underway recently in the House of Commons.

As a reminder, if this bill were to be passed, Canada's Border Services Agency would have the authority to record the full name, sex, date of birth and citizenship or nationality of "any person who is leaving ... or has left Canada," along with the date, time and point of departure and the other details of the travel documents that served as proof of identity.

We know that Daniel Therrien will continue to provide advice and recommendations as the draft legislation passes through the parliamentary review and we will watch the proceedings with great interest.

My office is also working with the federal privacy commissioner to determine how many British Columbians are affected by the massive Equifax breach. This breach affected 143 million Americans and approximately 100,000 Canadians.

In international matters, the OIPC is proud to continue its leadership role as secretariat for the Asia Pacific Privacy Authorities (APPA) – that's 19 authorities in 13 countries – and will cohost the next forum here in Vancouver this November with the Office of the Privacy Commissioner of Canada. The experiences gleaned from these information networks offer great insights for member regulators and we look forward to another great session with our international colleagues.

## GDPR/the Future

Looking further afield now… We're inching closer and closer to the enforcement date for the EU's General Data Protection Regulation, or GDPR. This ***could*** affect BC public and private organizations!

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.

And the stakes are high:

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**

What do you need to know, now, about the GDPR? Here are five interesting elements.
Some of these will sound familiar to you:

1. **Enhanced consent**
    - Clear, unambiguous, can't be bundled, granular. Must be as easily revoked as given

2. **Data portability**
    - Provided to you in a machine readable format

3. **The right to be forgotten**
    - You can request your data to be deleted.

    Just think for a moment what those two rights mean – data portability and the right to be forgotten – when taken together. You could under the GDPR, for instance, request all your fitbit data, ask them to delete it from their servers, and take that data and use it with another fitness tracker.

    Imagine the level of ownership this will give EU citizens over the monetization of their personal information.

4. **Right to object to automated decisions**
    - Right to ask for human oversight and underlying logic into how decisions are made.

5. **And mandatory breach notification**

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

BC will need to react, and it is our hope, with a new government in place in Victoria, that some of our recommendations for improvements to FIPPA and PIPA will be undertaken in coming months. In fact, I met with the minister, Jinny Sims, this past Monday to discuss our key legislative priorities.

So, what's next for the OIPC?

We are currently at work on an audit of WorkSafe BC's access to information and privacy management program policies and responses to requests and complaints.

We are also in the middle of an investigation into the over-collection of personal information by landlords, after receiving several calls each week from individuals who have been asked by potential landlords for too much personal information. This is an important investigation, as renters may be reluctant to assert their privacy rights at the risk of losing housing options.

And, we have recently launched an investigation into government compliance with s. 71 of FIPPA, which, if you don't have the Act memorized like I do, requires the head of a public body to create categories of records available **without** an access request.

We have reached out to 30 public bodies to see how they are complying with s. 71 and I look forward to sharing the results with you in the near future.

And finally, I am pleased to announce (for the first time, aren't you guys lucky!) an investigation into the collection, use and disclosure of personal information by political parties. I will be looking into whether the BC Liberal, New Democratic 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, as well as several privacy breaches by these parties.

Wow, that sounds like a lot of work to get done before I expire ;)

Well…It's been a real pleasure to speak with you this morning – and to have served as BC's Acting Information and Privacy Commissioner for these past 15 months.

I wish you all a very good conference and hope to have a chance to speak with you throughout the day. If we have time for questions, I am happy to take them.