Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

**CHECK AGAINST DELIVERY**

# SPEECH AT THE

# FREEDOM OF INFORMATION & PRIVACY LAW PROFSESIONAL DEVELOPMENT CONFERENCE

## JUNE 2, 2016

**ELIZABETH DENHAM**
**INFORMATION AND PRIVACY COMMISSIONER FOR BC**

Thank you very much. Hello, everyone.

I must admit that I am feeling wistful today, because this is my last formal speech before my term ends July 6th. It feels to me like the end of an era!

It's fitting, though — because the CBA was the first group I spoke to when I started this gig back in 2010.

There I was, shiny and wide-eyed, talking about what I hoped to accomplish in my six-year term…

Then, at the end of my speech… a Q and A session and a certain person at the back of the room raised their hand and said (innocently)…

What is your view of the workability of section 30.1 of FIPPA?

A vexing question to this day.

Those of you who followed the recent FIPPA review this year… will know that the data residency rules was one of the most debated and difficult issues the Legislative Committee grappled with.

In the end, the Committee decided to leave 30.1 as-is.

(By the way, that person at the back of the room… was Lorene Novakowski, a respected colleague among many of you that I have got to know well over the past six years).

I am sad to be leaving B.C.

I am a Richmond girl, after all.

And this is the best place in Canada to be working in access and privacy.

We have an active bar, who contribute so much to law reforms in this Province we have active and engaged media, respected academics, dedicated civil society groups that have reach beyond this Province …

Privacy and access to information issues are dynamic in our digital world, and this is a very specialized area of the law.

You are the legal experts – the interlocutors of our laws.

You help your clients — and the broader access and privacy community — understand the ins and outs of the legislation, implications of new rulings, decisions of the Courts.

And you have been a welcome support to the work of my Office.

But as much as I love being B.C.'s Commissioner… I feel the pull to greater power.

Like a moth to a flame… I am drawn to a new set of regulatory challenges.

It's an honour to be appointed the next Information Commissioner of the United Kingdom.

And the timing couldn't be better — there's a lot happening across the pond. ☺

The EU's General Data Protection Regulation, with its new compliance requirements and stronger enforcement, has been given final approval by European Parliament and will take effect after a two-year grace period.

Whether or not there is a Brexit – the UK must meet the Regulation's high bar for privacy and data protection.

Privacy Shield discussions continue to move along, albeit slowly.

Ensuring the Privacy Shield is fit for purpose is critical for US companies seeking to do business in Europe, but also for countries like Canada, where the European Court of Justice's threshold for privacy could call our adequacy into question.

And new UK surveillance laws are currently being debated in Parliament, which if passed will have major implications for privacy.

A debate I'll be contributing to in my new role.

There will be a steep learning curve. I'll be overseeing new laws – and navigating a new political culture.

But I love a challenge… and I look forward to sinking my teeth into some new files.

A question I am often asked these days:

What am I most proud of, in my 12 year-run as a privacy regulator in Canada?

It is impossible to pick just one case, one moment that stands above the rest.

But I can reflect on the broader outcomes of the work — where I think we have made a difference.

**Making a difference to the public**

I am proud of the files where our work made a difference to citizens.

The **Facebook investigation**, which I led as Assistant Privacy Commissioner of Canada — is one of the big ones.

The privacy controls some of us might take for granted today, were implemented as a result of that 2008 investigation…giving Facebook users around the world the ability to control their personal information, and how it is shared with third party apps, other users, and the platform itself.

Here in B.C., my office's broad-brush investigation into **police information checks** resulted in a province-wide policy changes…where mental health information, including police apprehensions and suicide attempts, was eliminated for all record checks…and non-conviction information ceased to be disclosed for all jobs outside the vulnerable sector.

For the thousands of British Columbians who require a police information check each year — that change made a huge difference… and lifted the burden of having to explain these sensitive details to a prospective boss.

And our **deleted email investigation**, released last October, prompted a landslide of media coverage and public concern.

But, more importantly, it prompted the Premier to commit to pass duty to document legislation and other key access to information policy changes.

These changes pave the way for clearer skies for public record keeping, greater accountability for citizens, and robust information rights – because records will be created and retained.

**Pulling back the curtain**

Another important place I believe we've made a real difference… is where our investigations pulled back the curtain on new technologies.

From automatic licence plate recognition, to employee monitoring and spyware…we've helped the public better understand these technologies and their impact on personal privacy.

The onus is on regulators to shine a light onto the far corners of a program, policy or issue on behalf of the public.

So that citizens can make informed choices, advocate for change, and contribute to public debate.

I am also proud of the important decisions the office has made – the orders, findings, and recommendations – that have moved the law forward.

I did a quick tally of all the reports and decisions we've published since July 2010.[1]

- 274 Orders and Decisions
- 35 investigation and special reports
- 2 audits

We've been a bit busy. ☺

Each of these rulings is important. But some stand above the rest.

Where we moved the marker on legal interpretation…or where we applied tried-and-true principles to new and emerging technologies.

I'm going to start with section 25 – arguably the most important interpretive change to FIPPA in recent years.

There were two phases to this work.

[1] NB: Current to May 23, 2016.

Phase one took place in 2013, when we launched a systemic investigation that assessed five cases …where it was alleged that public bodies should have disclosed information about a risk of significant harm to health and safety.

The main take-away from that investigation… was that the temporal urgency requirement was preventing public bodies from proactively disclosing information in the public interest.

Phase two… was our 2015 investigation report into the Mount Polley mine tailings pond breach.

I looked at both aspects of section 25 in this case – the duty to warn, and the duty to inform.

While I concluded that the government did not have in its possession any information that disclosed a risk of significant harm to the environment or to the health and safety of the public **before** the breach occurred, I did find there was a public interest in information about the tailings pond breach after the incident occurred.

However, the duty to disclose was not met, once again due to the interpretation of the need of temporal urgency.

After careful review, and due consideration to what legislators intended, I made a legal finding that re-interprets this section… so that urgent circumstances are no longer needed to trigger public interest disclosures.

Public bodies must tell citizens what they know… where it is clearly in the public interest to do so.

We are hearing from local public bodies and health authorities that public interest disclosures are starting to happen — for example, municipalities are contacting us about the application of s. 25 where soil testing revealed ground instability .

And it very much continues to be a live issue for our office.

The Environmental Law Centre recently complained to our office that the Ministry of Environment failed to meet its legal obligation to proactively disclose information about unsafe nitrite levels in Spallumcheen.

My public report on this matter will be released later this month.

The other really big file where our legal analysis and findings moved the marker was the District of Saanich's use of employee monitoring software.

I'm telling you… there has been more ink spilled by lawyers on this investigation report than any other I've issued as B.C.'s Commissioner.
It's been analyzed and scrutinized six ways from Sunday.

And that's a good thing.

The report represents, in my view, a nuanced approach to the very complex issues employers face when balancing employee privacy rights and the challenges of cybersecurity.

There are shades of grey here – and with this report we wanted to set out in clear terms where the line was, and how employers could balance IT security and employee privacy.

The Saanich investigation made headlines in B.C. and across Canada.

But the best part... was that it clearly and unequivocally set the record straight. Employees do not check their privacy rights at the office door.

Employees have a reasonable expectation of privacy at work, even when using a computer or mobile device supplied by an employer.

**New Technologies**

It's the big reports, like Saanich and Mount Polley, that make a splash in the media or in Question Period at the Legislature.

But there's a lot of really important legal work that happens in the trenches.

Two floors below the main OIPC offices, our adjudicators are working diligently to map privacy and access principles onto new technologies, as these issues filter through our complaints and appeals process.

I wish I could share all of their exemplary work – but I will limit myself to just a few cases.

*Open Data*

On the access side, the open government movement has grown in leaps and bounds in the past five years.

An increasing number of freedom-of-information requests are being made for data sets, rather than a paper trail.

I once had a reporter tell me that when they requested paper documents through FOI, 1 time out of 10 they would find a story. But when they started requesting data, they would find a story 9 times out of 10.

FOI requests for data are getting ever more sophisticated, in lockstep with the increasingly complex data collection and analysis tools of government.

It has been long established that government agencies must provide records electronically if they can do so relatively easily.

But the issues are getting more complicated.

Database dumps now result in tens of thousands – if not hundreds of thousands -- of lines of text, linked and cross-linked across data tables.

This can create complications when requests for records are made that include personal information.

For example, in 2015 we issued an order involving the BC Coroner's Service, where a journalist requested data on all deaths investigated by the Coroner over a 16-year period.

While the adjudicator determined that creating several electronic records (one for each table in the database) would not unreasonably interfere with the Coroner's operations…the records could not reasonably be severed, even with the assistance of automated data masking software… therefore the public body was not obliged to create them.

*Metadata*

Also in 2015, we issued an Order involving the Ministry of Technology, Innovation and Citizens Services, where an individual requested six months of email traffic logs of government employees housed on its servers.

The applicant wanted this metadata to create relationship maps showing the interactions between government employees.

The adjudicator concluded that metadata is personal information … because the email logs could reveal personal information about employees including work activities, hours of work and leave, and personal relationships.

The adjudicator also found that it was unreasonable to sever the personal information given the amount of time it would take to do so – even using automated technologies.

On the privacy side, adjudicators have taken on the use of new technologies in the workplace.

Through four binding orders, we set the terms of engagement for GPS technologies.

The GPS orders are significant because, first, we established that the data collected and used by the vehicle monitoring systems is in fact personal information.

Second, we set clear ground rules for what is acceptable and appropriate use of GPS in an employment setting.

For example, in Schindler Elevator Corporation the company could demonstrate that it was using the system to map routes, manage hours of work, and ensure that employees drive safely and lawfully -- all of which I concluded to be legitimate, reasonable business purposes.

These orders draw a clear line in the sand between these legitimate uses, which are periodic in nature… and illegitimate uses – like real-time surveillance.

And we also set the ground rules for appropriate notification of employees.

What do these cases tell us?

First, that our principle-based laws have the flexibility to address new and emerging technologies for both access AND privacy.

Second, that access and privacy by design will be critical going forward.

Public bodies are relying more and more on data-driven solutions to public policy problems.

Your clients, your organizations need to be thinking about how to facilitate access to information as they design these systems.

And having a complex database is not going to give you a free pass from having to respond to FOI requests.

Protecting privacy and facilitating access are of equal importance under the law.

Despite the retrospective tone of my comments today… I do still have a few big files left on my desk.

I've been burning the midnight oil to get these items across the finish line, including: A review of the City of Vancouver's access to information practices.

This is part of our new audit and compliance program. It's an examination of the city's practices and processes.

It is a thorough and detailed report. Look for that to come out this month.

The second item, which I mentioned earlier, is a public report about whether the Environment Ministry had a duty to disclose information about unsafe nitrite levels to the public.

So stay tuned for those two items.

In the meantime, I’m happy to answer any questions you may have.