Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

SPEECH TO

17TH ANNUAL PRIVACY & SECURITY CONFERENCE

FEBRUARY 5, 2016

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER FOR BC

Good morning everyone!

Thank you Cheryl for those kind words of introduction.

It is a great pleasure and a privilege to address you this early Friday morning.

Let me begin by offering up my congratulations to Bette-Jo Hughes and the Office of the Chief Information Officer, the Ministry of Finance, and to Greg Spievek and his team at Reboot.

You have once again succeeded in bringing together an impressive group of thought leaders in the world of security and privacy for this important summit.

Thanks for pinning Victoria on the privacy and security map.

***

There is a saying – “may you live in interesting times.”

Some would say that interesting times have been thrust upon privacy.

In my 10+ years as a regulator in three jurisdictions … I have NEVER seen so much public attention and debate about privacy.

There have been flashpoints in the past – most notably Edward Snowden's revelations about the scope of national intelligence gathering in the US.

But over just this past year, there has been a dramatic increase in public awareness, engagement, and ANXIETY about their privacy rights.

This has been driven by the fast-pace of new technologies and our big data world.

Technology permeates our economies, social interactions and intimate selves.

These technologies build communities. They save time. ☺ ??? They simplify our lives. ☺ ???

But there's a catch.
These super connected systems demand continuous access to us and our personal information, and are vulnerable to a host of new privacy and security threats.

While most of these technologies are OPAQUE to the vast majority of people … there is an increasing public AWARENESS that they are impacting our personal privacy.

When combined with recent important local, national and global events… it is little wonder those of us in this room find ourselves at the centre of some of the most compelling issues of our time.

The title of my presentation today hints at stormy weather – and the conference agenda also provides a barometer of the conditions we're all facing … cyber-security, big data, mobile apps, open source, **DISRUPTIVE** technologies, cyborgs, drones and the internet of things….

But if you look at these conditions from 30,000 feet, you will see yourselves on the leading edge of a system with the potential to be FAR less gloomy than the title of my speech suggests.

The two days of this conference are in fact part of an important dialogue that will help to track and shape the future path of privacy.

It IS an exciting time to be on this file when change is happening, day by day and hour by hour.

There is new regulation. There are new trade agreements, promising privacy commitments – AND a global recognition of the importance of privacy in our changing times.

The global economy is a vast interaction of multiple forces.

The digital economy requires data to flow across borders but different legal systems and cultural norms about privacy make this a complicated undertaking.

How do we bridge these differing regimes so that data can foster economic growth while respecting the privacy rights and expectations of citizens?

Events are unfolding on this front literally as we gather here today.

New Regulation

After a four-year marathon ... agreement has finally been reached on the reform of Europe's data protection laws.

The new General Data Protection Regulation – expected to be formally adopted in the coming months – retains and **expands** privacy rights … supporting a single digital economy across Europe.

Most crucially, it reminds people of their data protection rights and organizations of their data protection responsibilities.

The new regulation contains many compliance requirements AND stronger enforcement … setting a high water mark for data protection that will reverberate and affect privacy regimes around the world.

Safe Harbour

Another development with global significance is the **off-again, on-again** EU-U.S. Safe Harbour agreement…. The 15-year-old arrangement that governs data transfers between the European Union and the U.S.

The tempest began when Austrian activist Max Schrems alleged that the data he provided to Facebook was not adequately protected by the agreement.

This complaint shone a light on a defect of the basis for Safe Harbour… **Europeans lack redress rights under U.S. law.**

On October 6, 2015, the European Court of Justice invalidated the adequacy finding on which Safe Harbour is based.

This decision of course affects not only Facebook but also thousands of other U.S. companies that do business in Europe.
[sidebar: The decision may have impact on adequacy findings in other countries, including Canada]

Both sides need to find a link between these regions historically divided by different perspectives on privacy.

Just three days ago, we learned that negotiators have agreed on a framework for Safe Harbour 2.0.

This is a first step forward in bridging the regimes, but there are still challenges ahead. One thing we **DO** know is that there will be a stricter regime for U.S. companies.

TPP

Now, from the Atlantic to the Pacific….
Just yesterday, the Canadian government signed the Trans-Pacific Partnership, or T-P-P, along with 11 other nations. It will be the subject of significant Parliamentary debates and public discussion in the coming months.

Of course the deal won't be sealed unless there is a majority vote supporting it in the House of Commons.

Questions are being raised about the impact of this agreement on the data localization requirements in BC and Nova Scotia laws. While the TPP contains exceptions to the general requirement for the free flow of data, some worry that they could be difficult to rely on.

I am optimistic that our current privacy safeguards will be maintained through this trade deal.

When I talk to British Columbians, they want assurances that their data is shielded from foreign law enforcement orders.

The good news is that the BC government has recently committed to retaining current protections in our law.

Public Safety and Law Enforcement

And while the TPP is sure to be hotly debated in Canada, so are matters related to public safety and law enforcement.

At the heart of this fundamental debate… is a question: What is <u>proper oversight and supervision</u> of the surveillance activities of national security and law enforcement agencies?
We learned just last week that CSEC, Canada's electronic spy agency, violated privacy laws and that CSIS obtained taxpayer information from the CRA without a warrant.

This is further evidence that far more robust statutory, AND parliamentary oversight is necessary.

I do not underestimate the challenges posed by international terrorism, particularly after the Paris, Yemen and other attacks last fall.

However, we need cool heads to carefully analyze what information security services now have — and how they use it — before we extend to them any further access to our private information.

What we must avoid at all costs are knee jerk reactions. I am very concerned, for example, about recent suggestions that encryption services for consumers of online services be compromised in the name of security.

Some are now calling for backdoors that would give law enforcement access to encrypted data. The trouble is, you can't have it both ways – the same door could be opened by the bad guys.

The security imperative, either at the national or local level, must not close down the debate about privacy rights and obligations.

RCMP Commissioner Bob Paulson recently suggested that "privacy has become the crusade of those who would have us live in their textbooks".

You can imagine how I feel about this statement. ☹ PAUSE

What has worked well in the BC environment is an open and consultative discussion between police services and my office. On many files, we have been able to find the balance — determining where the public interest lies in the use of new technologies in programs like automated license plate recognition, police information checks, body worn cameras, to name a few.

Police and privacy commissioners need to respect one another's mandates and the public's expectations that we are able to work productively through issues as they arise.

Information Rights in BC

That trust also extends to information rights. As you may have noticed, they have also been on the front burner -- and the front page – here at home.
A legislative review of our public sector law is well underway. And the timing couldn't be better.

If there was ever an opportunity to ensure our laws have the flexibility, the tools, *and* the muscle to address the challenges of big data and new technologies, and provide meaningful oversight of information rights for citizens…

…now is the time.

We have an opportunity to respond to these national and international forces… and ensure that our laws can endure.

There has been a great deal of interest in this review. By the deadline last week, the Special Committee of the Legislature reviewing the Act had over 120 submissions in hand.

In November, my office set out our proposal for changes to the law.

Chief among them is **Mandatory Breach Notification for the public sector.**

We trust public bodies with our most sensitive personal information. Health records, tax data, financial information, and data about our children… the list goes on and on.

It seems as though every week, the public learns about a new data breach involving lost hard drives, stolen laptops, personal information accidentally posted online, Instagram postings of private health procedures, or employees 'snooping' in electronic records.

Privacy breaches carry a human cost.

They put individuals at risk for identity theft and serious reputational harms not to mention loss of confidence and trust in government.

The size of these breaches can be staggering. Last Thursday, I released a report about a breach involving a lost portable hard drive containing the educational data of **3.4 million individuals**.

Information assets, particularly the personal information of citizens, deserve the same respect, rigour and control as the management of financial assets.

The government of BC has a very long tradition of strong financial management, which includes specialized training, record keeping, and a robust audit function, so a loss, for example, of $3.4 million would be highly unlikely.

Breach reporting in BC is currently voluntary. My office receives reports of what we believe are only 1% of all privacy breaches that occur within the larger public sector.

Our current voluntary regime means there is no clear threshold for reporting to my office, no consistency in when breaches are reported to affected individuals.

The public policy purpose behind reporting breaches is not punitive, nor is it intended to be a shame and blame regime.

Mandatory reporting of breaches will drive good tracking of personal information assets.
It will focus attention and investment in IT security… and that's a good thing, for some of you in the room here today. ☺

Duty to Document, and oversight of records destruction

My second major recommendation for reform stems from my findings in our investigation report "Access Denied," released in October 2015.

The main finding in this report and in previous reports … is that freedom of information rights can only be exercised when public bodies create and keep records of the key actions they take and decisions they make.

I believe a legislated duty to document and oversight of record destruction are critical elements of good records management, accountability and good government.

I am not alone in this belief. Information Commissioners are hearing these concerns across Canada, and conducting their own investigations into document destruction.

And just last week, the Commissioners collectively called upon their respective governments to create a legislated duty requiring public entities to document matters related to their deliberations, actions and decisions.

It is clear to me that British Columbians care deeply about this issue.
Results from an Ipsos survey commissioned by the BC Freedom of Information and Privacy Association, released just this week, indicate that an overwhelming **96% of British Columbians** support duty to document, along with **84% favouring penalties for destruction of documents**.

Some documentation **is** taking place now in B.C. — but if we were to take a snapshot today … it would be an **incomplete** picture of the 'what' and 'why' of government decision-making.

I was pleased that government has accepted all the recommendations in my investigation report.

Premier Clark has committed to passing duty to document legislation, stating that "It's not a question of **WHETHER**; it's a question of **HOW**."
I am optimistic that clearer skies are ahead in regard to public record keeping in this province.

These legislative changes would once again make BC a leader in information rights in Canada.

Conclusion

MY JOB is to uphold privacy and information rights while ensuring economic growth and social benefits.

But my office can't do this alone.

Privacy is a team sport.

Effective regulation requires engagement **with** the public sector, **with** industry, **with** civil society, and **with** the public at large. Each one of you in this room has an important role to play in this critical process.

So when you need to engage with my office, I hope you know that my door is always open. I truly appreciate the opportunity to have these important discussions.

So we DO live in interesting times. And that isn't likely to change any time soon.

But when you consider **ALL** that has occurred over the past year we **ARE** making progress.

We **CAN** and **MUST** stay the course to ensure our privacy and information rights are strengthened in the digital age.

Thank you. Enjoy the rest of the conference!