CHECK AGAINST DELIVERY

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

SPEECH AT THE

6TH EUROPEAN DATA PROTECTION DAYS

APRIL 25, 2016

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER FOR BC

It's a pleasure to be here -- among old friends and new -- to talk about accountability in my capacity as Information and Privacy Commissioner for British Columbia, Canada.

Over the next 15 minutes, I'll describe accountability and how it's being applied in Canada. I'll also speak to accountability's influence on privacy and data protection in Europe. Finally, I'll address what the future holds for accountability. I'll leave a few minutes for questions at the end.

What is accountability?

Let me start with a broad outline of accountability.

Accountability holds data controllers ethically and legally responsible for the processing of personal data.

The onus is on the company to understand the risks that they create for others, and to mitigate those risks.

In practice, accountability refers to a framework used to build a culture of privacy that pervades an entire organization.

Accountability encourages an investment in privacy fundamentals UPFRONT…

BEFORE systems are built, and the foundations of data processing are laid…

…rather than notifications after-the-fact when the data flows are turned on.

Of course, in order for accountability to work, there must be a legal authority to hold the company to account. This role falls traditionally to data protection supervisors.

Accountability in Canada

I'm proud to say that Canada was the first jurisdiction in the world to write accountability into law.

The *Personal Information Protection and Electronic Documents Act* sets out fundamental accountability requirements, including:

- A statement of responsibility;
- Designation of a privacy officer;
- Policies and processes to put the privacy **principles** into effect; and
- Ensuring equivalent protection for outsourcing arrangements.

Many of the same requirements are contained in similar privacy laws of the provinces of British Columbia, Alberta and Quebec.

Since the federal law (PIPEDA) was adopted in 2000, Canadian Commissioners have worked to put substance on the bones of accountability through investigations and enforcement work.

Getting Accountability Right

But by 2010 it was clear that, with the exception of the financial services sector, many businesses did not understand accountability, or how to implement it.

Canadian Commissioners also observed a "paperwork of privacy" syndrome, where policies collected dust on a shelf. No privacy officer. No training. No monitoring. No clear line of reporting. No risk assessments….

In other words, no awareness of privacy across the organization.

Channeling the good work being done around the world – in particular by the Global Accountability Dialogue that met over a number of years in Europe – I collaborated with two of my Canadian Commissioner colleagues to write a policy paper that outlined our expectations for accountability.

To reinforce the fact that accountability should be <u>foundational</u> and not a bolt-on solution, we describe accountability as a "privacy management program."

The intention for the paper, *Getting Accountability Right with a Privacy Management Program*, was to provide a **blueprint** for organizations… to provide the building blocks of accountability – starting from organizational commitment, followed by program controls, and then ongoing monitoring, assessment, and revision.

It's a blueprint that works for organizations of all sizes, as well as those that process large and small amounts of personal information. In British Columbia, I also wrote a companion document that extended accountability to the public sector.

With this guidance, Canadian Commissioners put the private sector on notice about our expectations with respect to privacy management.

Applying Accountability to Investigations

Then we began to apply the privacy management framework in enforcement actions.

In British Columbia, we've assessed accountability in a number of high-profile investigations, including:

- the smart meter and smart grid program of a large power company;
- the use of facial recognition technology by an auto insurer; and
- an employer's decision to implement monitoring software on staff computers.

These investigations included a review of the **technical** breaches of the law, but more importantly, they also included a broad examination of the organizations' privacy management practices.

All of them complied with my recommendations and made the required investments in privacy management.

This regulatory approach has a cascading effect – we've seen the adoption of comprehensive programs in peer companies.

For example, following the release of a public report about a data breach at a B.C. university, we saw significant and sustained investments in privacy management at other major universities in the province. .

Accountability Frameworks Around the World

Since the Canadian paper was published in 2012, other DPAs have also issued accountability guidance, including my colleagues in Hong Kong, Australia, and Columbia.

The Article 29 Working Party and CNIL have also issued accountability guidance.

New Developments in Canada

And accountability continues to evolve in Canada.

In British Columbia, a Legislative Committee recommended that B.C.'s law be amended to **explicitly** require organizations to implement privacy management programs. These programs would be tailored to the structure, scale, volume, and sensitivity of the organization's operations. The Committee also recommended a change in the law to require organizations to stand ready to demonstrate their programs to the Commissioner, and mandatory breach notification requirements, a key element of effective privacy management.

This is a significant step forward.

Incentives

The incentives for you to invest in accountability are greater than they have ever been.

In a world of ubiquitous computing, big data analytics, and cloud computing, it is not enough for a business to simply comply with the narrow letter of the law.

Today, there must be a meaningful investment in data protection; to build a living and breathing privacy model that underpins the entire organization.

Accountability is **so** important to client relations and customer retention. People expect companies to be accountable for how they process personal data.

Break their trust, and you will lose their business.

The regulator's gaze is another powerful incentive. If I investigate a complaint and don't see any evidence of a privacy management program – no privacy officer, no policies, training, or controls -- it's likely I will pursue a fulsome enforcement action.

On the other hand, if we get a complaint, and the company can show it has a full program, that could be a mitigating factor in my approach.

But perhaps one of the greatest incentives… is the synergy between an accountability approach… and recent developments in data protection in Europe.

GDPR and Accountability

The new General Data Protection Regulation is steeped in accountability --- and it has teeth.

The general accountability requirements include Article 5, which sets out the responsibilities of data controllers to adhere to core privacy **principles**.

And to compliment this is Article 24, which requires controllers to implement measures and policies for compliance, with attention to the "nature, scope, context, and purposes" of processing. **Sound familiar?**

Article 25 requires data protection by design and default.

More specific requirements that promote accountability lie throughout the Regulation -- the designation of a Data Protection Officer, data protection impact assessments, and keeping records of processing activities.

The Regulation is also explicit that data controllers may use codes of conduct and certification mechanisms for demonstrating compliance.

As with any new regime, there will be a learning curve.

The risk is that businesses and public bodies will fail to connect the dots. Data controllers may see the Regulation as disjointed, or that it simply expresses a need for better record keeping.

What the Canadian experience has taught me, though, is that a systems approach is best.

Our guidance provides a blueprint for how to structure privacy management, with the flexibility to address any new requirements that may come on-stream.

And, from regulator's perspective, accountability provides consistency in the way those requirements are fulfilled. It provides certainty as to what the regulator expects.

But it's not just about seeing the bigger picture with the GDPR.

Accountability was included in APEC's policy framework back in 2005. BCR is an accountability framework, a full blown privacy management program and not just a transfer mechanism. Very recently, explicit accountability requirements were also embedded into privacy laws in Mexico and Columbia.

Other regulators around the world, including the UK ICO and the FTC have required companies to implement a comprehensive privacy management program in response to enforcement actions and consent decrees.

Accountability is a privacy bridge for global companies.

The connection has to be made and must be fleshed out in the GDPR implementation and beyond, by both regulators and data controllers.

Transition to Ethics/Panel

In closing, I believe accountability has a bright future.

There is a growing global consensus that privacy compliance demands a comprehensive approach.

We're also seeing a proliferation of organizations promoting accountability – including the Canadian company Nymity, with their tools and metrics, the Centre for Policy Leadership and the Information Accountability Foundation.

But before I move to questions, a word about accountability and ethics.

Like accountability, an ethical approach to data cannot be bolted on – it needs to be a part of the company's overall systems approach to how it manages and processes personal data.

Thank you. I am open to any questions or comments that you may have.