Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

CONVERTING ACCOUNTABILITY INTO CREDIBLE BUILDING BLOCKS FOR CONSUMERS AND REGULATORS

PRIVACY LAWS & BUSINESS
27TH ANNUAL INTERNATIONAL CONFERENCE
CAMBRIDGE, UK
JUNE 30, 2014

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER FOR BC

Thank you, Stewart. It is a pleasure to be here. I have followed Privacy Laws & Business over the years and am very pleased to be here to talk about work underway in Canada on the accountability front.

I am very enthusiastic about comprehensive privacy programs and the importance of an accountability approach to data protection—but I do realize that this subject can sound a bit like reminding the public about the importance of eating a balanced breakfast! So I will start with some history and end with real life examples of accountability in practice and enforcement.

Before I begin, a few words about my home province of British Columbia. BC is on the west coast of Canada, a province of 5 million. We have ten provinces and three territories, and a division of powers between federal and provincial governments. Unlike the UK, we are not an island, we happen to have a giant neighbour to the south.

As a provincial privacy commissioner, I oversee public and private sector privacy laws including the privacy practices of businesses that aren't based in BC but have a real and substantial connection to our province. Within Canada, Privacy Commissioners work together on joint investigations, education and guidance. We pull back the curtain on new technologies to shine a light on a company's programs, policies and business model to assess whether appropriate protections are in place.

But BC is a little bit special. While other parts of Canada are focused on the EU or the United States, BC is the gateway to the Pacific Rim. Trade connections with Asia are vital to our economy. These geographic and economic ties have promoted positive working relationships and information sharing between Canada and other privacy authorities in the region. My office is an active member of the Asia Pacific Privacy Authorities. We are hosting Canada's first ever APPA meeting December 2nd and 3rd in Vancouver.

Singapore's new *Personal Data Protection Act* is based on Canada's federal privacy law. And the Hong Kong data protection authority has translated and adopted Canadian-authored accountability guidance for private companies in his jurisdiction. These ties can only make us stronger—after all, privacy is a team sport, and we have to work together—regulators, privacy officers, governments, and businesses—to achieve meaningful and lasting privacy protections in the digital age. I'd like to think that BC and Canadian Commissioners are pathfinders—in that we emphasize practical tools and incentives to make a lasting commitment to comprehensive privacy management through accountability programs—which is the focus of my speech today.

Let me start by talking about what I mean by accountability. Just as a free and autonomous individual is responsible for their own actions, accountability holds data controllers ethically and legally responsible for the processing of personal data. The onus is on the company to be aware of, and comply with, the law rather than relying on a regulator to verify compliance.

But accountability is also much more than that. It is a powerful tool to encourage companies to commit to building a culture of privacy that pervades the entire organization. Accountability is a systems-based approach, where an investment in privacy fundamentals is encouraged before systems are built and the foundations of data processing are laid rather than notifications after-the-fact when the tools are in place and the data taps are about to be turned on. Of course, in order for accountability to work, there must be an authority to hold the company to account. This role falls traditionally to Commissioners/data protection supervisors.

However, the public plays an increasingly important role. Individual participation is an essential element of accountability. Citizen demands for accountability—be it Europe vs. Facebook, social media campaigns against online spying, or class action lawsuits against companies suffering data breaches—are on the rise and are an important incentive for companies to make a commitment to comprehensive privacy controls.

Let me also state what accountability is not.

Accountability is not a new concept

Way, way back in 1980, the OECD released its data protection guidelines that said:

> A Data controller should be accountable for complying with measures which give effect to the principles stated above. (OECD 1980, s.14)[1]

Since that time, accountability has flourished, from its inclusion in the 2005 APEC policy framework (APEC, 2005 s. 26), to its embedding in privacy laws, first in Canada's private sector law PIPEDA and then more recently in Mexico and Columba's laws. In 2013, the OECD amended its Privacy Guidelines to elaborate on implementing accountability by specifying that data controllers should implement privacy management programs. And the Global Accountability Dialogue, (led by the Information Accountability Foundation), a multiyear initiative involving DPAs, global companies, academics and stakeholders began with discussion about the adoption of accountability and how to measure the presence of a program. The discussion has moved on to define effective demonstration of sound data governance.

Accountability is not a Trojan horse to eliminate notice and choice

It's a long-standing global movement with the aim of providing lasting and meaningful compliance and commitment to privacy principles. In my view, notice and choice have a big part to play in accountability. The challenge is to make transparency and individual participation work when purpose is complicated by analytic processing. What accountability does require is that data controllers can't translate risk to individuals simply by getting consent.

Accountability is not at odds with the EU's privacy framework

There have been several attempts to introduce accountability language in the General Data Protection Regulation. In 2010, an Article 29 Working Party Opinion called for a new provision that would cement the concept of accountability into a revised Directive. (Article 29 WP, 2010, s. 74) This proposal sought to require companies to implement accountability measures, and to demonstrate compliance and commitment upon request, as highlighted here.

[1] Most recently, in 2013, the OECD amended its Privacy Guidelines to elaborate on implementing accountability by specifying that data controllers should implement privacy management programs. (OECD 2013, s.15)

In 2012, the European Commission proposed to address the principle of accountability in the General Data Protection Regulation. (EC, 2012 s.60) Again, the fact of an organization's responsibility for privacy compliance, and the requirement to demonstrate compliance to an authority, are recognized here. Also in 2012, the European Parliament's draft report amended the Commission's proposal to more explicitly mention the concept of accountability, and also clarified that this includes only an obligation to be able to demonstrate compliance on request. (European Parliament, 2012)

Obviously the wording of the Regulation is not finalized, but the push for accountability is not waiting for the new regulation. Any company that has a BCR by definition has an accountability program. And Working Party 29 is churning out policy papers left and right that go beyond the law as it exists today – papers on legitimate interests, compatible purpose, anonymization, and the right to be forgotten all require accountability to be compliant.

I would like to turn now to a discussion of how we are implementing accountability in Canada. Some of you may know that Canada was the first country in the world to write accountability into its privacy laws. The laws in Canada are consent based and accountability based. The bottom line is that people should be protected. Adopted in 2000, PIPEDA lists accountability first among 10 privacy principles. Because provincial laws have been declared substantially similar to PIPEDA, they too are interpreted to include accountability provisions.

By the late 2000s, Canadian Commissioners recognized the need to take the principle of accountability from theory to practice. With the exception of the financial sector, it was clear that many businesses had no clue what accountability was, or how the legal requirement should be implemented. We also observed a lack of meaningful commitment to privacy on the part of companies who knew there were privacy laws. They could talk the talk, but they weren't walking the walk. And among some businesses, we saw evidence of a "paperwork of privacy" syndrome—a policy here and there collecting dust on a shelf—but they had not invested in a culture of privacy. This state of affairs suggested to us that there was a need for concrete guidance and compelling incentive to follow it.

Channeling the good work being done around the world on accountability, and leveraging the legal requirement of accountability in Canadian law, three of Canada's Commissioners got together to create a guidance document called "Getting Accountability Right with a Privacy Management Program". It is tailored to the private sector and outlines the three stepping stones to comprehensive privacy controls for your business.

The key starting point is organizational commitment—that means tone from the top, and a genuine commitment to invest in privacy that is communicated by the head of the company. The foundation includes creating a Chief Privacy Officer role. This person should sit at the executive table and should be empowered to lead the privacy agenda for the business. Once this foundation is laid, program controls are

necessary, followed by ongoing assessment and revision—this is critical in light of changing threats and risks. The key is that privacy and data protection is not a one-time investment, or a one-off activity. It is an ongoing, evergreen process that must be done in a holistic way.

With this accountability guidance, Commissioners are raising the bar for what it means to be compliant. In a world of ubiquitous computing, big data analytics and cloud computing, it is not enough for a business to comply with the narrow letter of the law or technical provisions of the Act when a new tool or technology is introduced.

In an accountability framework, legal compliance involves a foundational commitment to privacy, and a deliberate and meaningful investment to build a living and breathing privacy model that has the flexibility to address new technologies, and the ability to comprehensively reduce the risk of costly privacy breaches, data spills and accidents.

Data processing is complex; companies need to have a program that reaches beyond compliance. Accountability may be the smartest strategy you have to future-proof your data-handling practices. When developing this guidance document, Commissioners spent a lot of time talking about the incentives for businesses to comply. There are the financial incentives—a penny now saves a pound later, especially where mass data breaches are concerned.

The path to compliance is laid out very deliberately—Commissioners have set out the roadmap to follow, step-by-step. The guidance is consistent across virtually the entire private-sector, making it easier for businesses to understand their accountability obligations under the law. It is also easier for a regulator to acknowledge that an “oops” has occurred when a comprehensive program is in place rather than incidents caused by a systemic failure—incidents that could have been fixed with an accountable approach.

Of course, the eagle eye of a regulator is also a compelling incentive. In British Columbia, we are applying this framework to our in-depth investigation reports. Some examples include the use of facial recognition technology by a government-owned auto insurer, the smart meter and smart grid program of a large power company, and a privacy breach involving an online gambling site.

All of our investigations looked at specific technical breaches of the Act, as well as the company's overall privacy practices. We achieve this through a small teams approach with investigators, technical experts and policy analysts working together on systemic files.

First, we collect the raw materials by reviewing detailed documentation including privacy impact assessments and security threat risk assessments. We go on site visits to examine systems in operation. We ask questions of front line staff as well as project leaders, and we peek under the hood at systems architecture. We evaluate the program from all angles; measure it against the organization’s privacy obligations

as well as the accountability framework. At the end of the process, our team meets with the executive team to tell them how they did.

We also release a detailed public report that includes not only our findings and recommendations, but also a plain-language account of how the organization is managing personal data, including type of data it's collecting, policies and training, and our assessment of security and privacy controls.

In all cases so far the companies have complied with our recommendations and have made the required investments in comprehensive privacy management investments that could have prevented the privacy problems we saw in our investigations. In addition, after the public reports, we've seen a cascade effect—adoption of comprehensive programs in peer companies.

We are seeing accountability being implemented on a proactive basis as well as in response to some of our more targeted work in specific sectors. We've seen examples across health care, professional regulatory agencies, universities and government-owned corporations. There are also private companies and consultants cropping up to assist organizations to implement accountability, using our paper as the roadmap.

In closing, while building a privacy culture sounds really, really tough, the solution is actually quite easy. Accountability is a framework ready for you to adopt, and will put your company ahead of the curve when it comes to the changes to the EU Regulation. And no matter where you are in the world, know that regulators are turning their minds to the principle of accountability and the demonstration of compliance.

I encourage you to embrace accountability and consider how it can be made to work for you. The accountability guidance is available from our website.

Thank you so much for your attention and I'd be happy to answer any questions that you have.