Office of the Information and Privacy Commissioner of Alberta

CHECK AGAINST DELIVERY

Cybersecurity from a Privacy Regulator's Perspective

Jill Clayton, Information and Privacy Commissioner

Keynote Presentation at the 2016 Cyber Summit hosted by Cybera
October 27, 2016 | Banff, Alberta

Thank you for the invitation to be here today and to share some of my thoughts on cybersecurity from a regulator's perspective.

As you know, my name is Jill Clayton and I'm the Information and Privacy Commissioner of Alberta.

The topics that will be addressed at this conference reflect much of what my office is experiencing. Open information, big data and the Internet of Things are matters of interest to information and privacy regulators around the world. And as we near the end of Cyber Security Awareness Month, it gives us an opportunity to reflect on where we've been and where we're going in the coming months.

The diversity of topics to discuss over the next two days are timely and forward looking – from privacy protection for genetic information to artificial intelligence and big data – and the interplay between new technologies and the law all require lots of attention.

I always enjoy attending conferences such as this one as they reinvigorate a sense of purpose for the role my office plays. There really isn't a dull moment when

considering the multitude of topics encompassed within cybersecurity and the protection of privacy.

In my comments this morning, there are a few topics I want to explore in a little more depth, including:

- **The Internet of Things.** Specifically, I will review the results of a recent global privacy sweep on connected devices that found nearly 70% of policies don't adequately inform consumers about how their personal information is being used. This will also provide an opportunity to speak about connected cars and our office's work in reviewing and accepting privacy impact assessments for usage-based auto insurance programs in Alberta.

- **Privacy Breaches.** As our office always says, "It's not a matter of if you'll experience a breach, it's when." Alberta remains the only private sector jurisdiction in Canada with mandatory breach reporting and notification provisions in effect. I will briefly explain the role my office has when reviewing breach reports submitted to the office and my power to require businesses to notify affected individuals. Further, I will outline some of the major trends we're seeing, which I'm sure will reinforce some of your thoughts on this topic.

- **Privacy education.** As we know, the law struggles to keep pace with technology but so too do educational institutions. Recently, a privacy competency framework for school students was developed and released at the International Conference of Privacy and Data Protection

Commissioners. My office has a supporting role in a comprehensive project called “The eQuality Project”, which is being led by criminologist Valerie Steeves and law professor Jane Bailey from the University of Ottawa. This seven-year research project was awarded funding from the Social Sciences and Humanities Research Council, or SSHRC, and is looking into issues of big data and the privacy implications of technology in classrooms and will be identifying evidence-based policies that promote healthy relationships and respect for equality online.

- **Privacy law from a European context.** As we look ahead and consider what may happen in the world of cybersecurity, we must also be aware of the developments in Europe with respect to the *General Data Protection Regulation*, or GDPR, that comes into force in 2018. This really will shift the landscape of privacy law and policy. The GDPR has made privacy law across Europe stricter and enhanced the protections for Europeans’ personal information in many areas, including around consent, accountability and privacy management frameworks, breach notification, and privacy impact assessments.

Internet of Things

But first, I’ll start with the Internet of Things, or IoT. I have seen estimates that peg the number of connected devices at around 6 to 15 billion, with between 20

to 30 billion devices expected by 2020[1]. Needless to say, it's a topic worth exploring!

This year, my office participated in the Global Privacy Enforcement Network's, or GPEN's, annual privacy sweep, which focused on the Internet of Things.

For those of you who might not be aware, the GPEN is an informal network of 51 privacy enforcement authorities in 39 nations around the world. It was established in 2010 on a recommendation by the Organisation for Economic Co-operation and Development to foster cooperation among privacy regulators in a globalized economy.

This privacy sweep of the Internet of Things reinforced three things for me. One, the ingenuity and advancement of these technologies is truly remarkable, and in many ways these devices provide a variety of benefits. Just think, connected heart monitors or insulin pumps are helping to save lives. Two, the implementation of such devices is far outpacing privacy law and policy. And three, these devices pose risks in a cybersecurity context.

When speaking about IoT we really are talking about surveillance devices in one way, shape or form. And what we and other regulators learned from the sweep was that many of these devices do not adequately tell consumers how their personal information is being collected, used or disclosed. This provides pause for me and fellow regulators, but also provides opportunity for us to identify best practices, trends and gaps in understanding for businesses and consumers.

[1] http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

Internationally, the report showed that of the more than 300 devices reviewed[2]:

- 59 per cent failed to adequately explain to customers how their personal information was collected, used and disclosed
- 68 per cent failed to properly explain how information was stored
- 72 per cent failed to explain how customers could delete their information off the device, and
- 38 per cent failed to include easily identifiable contact details if customers had privacy concerns

Fortunately, I'm happy to report, of the devices my office reviewed and the policies analyzed in Alberta, privacy issues and risks were adequately communicated. This included usage-based auto insurance programs and smart metres used by utility companies for billing.

With respect to usage-based auto insurance technologies, I should note that earlier this year insurance companies were permitted to offer UBI policies to customers in Alberta. Before being allowed to enter the Alberta market, the Superintendent of Insurance (Alberta Treasury and Finance) requires insurance providers to submit privacy impact assessments to my office for review and acceptance prior to implementation. In anticipation of this policy decision, my office developed *PIA Guidelines for Insurers Looking to Implement Usage-Based Insurance Programs in Alberta*[3].

[2] https://www.oipc.ab.ca/news-and-events/news-releases/2016/alberta-participates-in-global-privacy-sweep-on-internet-of-things.aspx
[3] https://www.oipc.ab.ca/media/650845/Guide_PIA_Guidelines_for_Insurers_UBI_Jan2016.pdf

To date, three such PIAs from insurance companies have been accepted by my office.

The world of IoT brings a number of other cybersecurity considerations into focus. Security patches are one thing on an operating system or within a network, but they're entirely different for a refrigerator or connected car. What policy implications do these have on reasonable safeguards for the protection of personal information, for example? What role must businesses play in this protection of consumers? Where do legislators fit in? And where do I and other privacy regulators need to provide guidance? With the rapid pace of technology, I expect the answers to these questions will be equally dynamic and thought provoking.

As we saw just last week, it is speculated that the attack that brought down or interrupted service to more than 1,200 websites, including Amazon, Netflix and Twitter, was driven through internet connected devices[4].

Privacy Breaches

While we continue to consider ways to grapple with the policy implications for IoT, we are also faced with the daunting task of mitigating the impact breaches are having in all sectors.

And, as we have seen recently with prominent internet and social media companies, any organization, no matter how sophisticated, is vulnerable to these sorts of attacks. As my office says in our breach workshops, "It's not a matter of if you will experience a privacy breach, it's when."

[4] http://www.wsj.com/articles/web-attack-stemmed-from-game-tactics-1477256958

My office is receiving nearly one breach report for every day of the year. In other words, we received more than 300 breach reports in the last year alone!

Most come from the private sector due to mandatory breach provisions in legislation, but we have seen a substantial increase in the health sector in anticipation of upcoming breach reporting provisions under the *Health Information Act.*

In the public sector we see significantly fewer breach reports but if Newfoundland and Labrador is any indication we would receive a lot more if there were mandatory breach provisions under the *Freedom of Information and Protection of Privacy Act*.

Newfoundland is the only jurisdiction in Canada to have mandatory breach provisions for public sector institutions. In the most recent quarter from July to September, 41 breaches were reported to the Commissioner in Newfoundland[5]; whereas, my office received less than 40 in one fiscal year. Just to place that in perspective, Calgary is home to twice the population of all of Newfoundland.

The types of breaches are varied and usually have a technology component.

For example, we all too often see employee "snooping" cases in the health sector. This is when healthcare employees have been caught looking into another person's health history without a legitimate reason to do so. In some cases, my office will pursue offence investigations depending on the circumstances. Over the past 18 months, four cases have resulted in charges being laid for allegedly knowingly accessing health information in contravention of legislation. And I have

[5] http://www.releases.gov.nl.ca/releases/2016/oipc/1017n06.aspx

publicly stated before that right now we have close to 30 such cases flagged as potential offence investigations.

We also see human error when mailing or emailing personal information to the wrong hands or inboxes. This is, and has always been, a common cause of breaches.

As is lost and stolen mobile devices. Just last year, we saw roughly 10 or so breach reports related to unencrypted mobile devices being lost or stolen that contained personal information. These occurrences simply should not be happening considering the widespread availability and ever-reducing cost of encryption technology. It's been several years since the office first called on organizations in all sectors to encrypt devices to mitigate harm when laptops or phones containing personal information are lost or stolen[6].

In addition to the breach trends I've just noted, we are also seeing an increase in breaches that result from hacking, malware or phishing. In multiple cases, hackers installed malware on organizations' websites or gained unauthorized access to customer databases, specifically targeting financial and credit card information of customers.

We've also seen the rise of ransomware in its different forms in Alberta. In one case, a casino's information systems were hacked and the information at issue was held for ransom. In other situations, however, systems were locked down until a ransom payment was made.

[6] https://www.oipc.ab.ca/news-and-events/news-releases/2010/seven-stolen-or-lost-laptops-in-one-month,-no-encryption-commissioner-says-%E2%80%9Cwhat-the%E2%80%A6%E2%80%9D.aspx

To respond, in March 2016 we published a one-page *Advisory for Ransomware* that we posted on our website at www.oipc.ab.ca.

We have also seen an increase in another cybersecurity threat which involves unauthorized individuals posing as a CEO or other senior executive asking HR personnel or another administrator within the organization to send highly sensitive personal information in, for example, a spreadsheet. Only after the email is sent does the organization discover that the information was sent outside the organization to an unknown, unauthorized third party.

In one of these cases, the membership list of an association was sent to an unauthorized individual. The reason I mention this is that it relates to an openness and transparency angle of breach response – and that is notification of affected individuals. In this case, the organization posted a video apology on its website and on a social media site. I believe this was the first time we had seen a video apology that was distributed widely.

What we have found in our work in this area is that open, honest and transparent notification greatly reduces anxiety and often the number of complaints my office will receive in relation to a breach. In our experience generally, the less people know, the more likely they will be calling us to better understand what options for recourse may exist and the more likely they are to make a complaint.

And, as Harvard Business Review, has recently commented, the more preparation for a breach, the better off an organization is[7]. Since hackers are seemingly always

[7] https://hbr.org/2016/10/your-company-needs-a-communications-plan-for-data-breaches

one step ahead, breach response plans need to be in place well in advance of any incident occurring.

Privacy Education

Like everything else I've touched on, the next topic I want to speak to is in constant flux and development – and that's privacy education and awareness.

This is an area where everyone seems to be on the same page – that we need more of it to teach students how to safely navigate their online world – but at the same time feel as though we're never catching up – new tools, games and gadgets keep coming up with new ways to collect and share information often without knowing exactly how that information is being collected, shared and monetized. And what I've heard anecdotally is that it's not so much that kids have changed – no, "kids these days" are no worse than our cohorts in years past – but the environments in which they're communicating have given rise to a number of the issues around cyberviolence and online harassment.

Identifying and facilitating opportunities to educate youth on access and privacy issues is part of my office's organizational plan. My office participates in a School at the Legislature program put on by the Legislative Assembly of Alberta that allows students in Grade 6 to learn about the legislative process and the various legislative functions, including legislative offices. My office's focus in these presentations is to help students gain an understanding of what personal information is and the digital footprint they develop over time.

My office also collaborates with federal, provincial and territorial information and privacy regulators across Canada on a working group to discuss issues surrounding educating children and youth about privacy issues.

This focus on privacy education led my office to provide support to The eQuality Project. As mentioned, this project was awarded a grant by SSHRC. It is a seven-year project that is quite exciting to be a part of. Essentially, it's looking at the interplay between big data and technology in classrooms and how it impacts privacy. It has hopes to "reinvigorate" the debate on cyberviolence and develop policies to promote safe and healthy online relationships[8].

To that end, our office has agreed to co-host an event in the coming months to discuss these very issues. The eQuality research team will be traveling to Edmonton to lead a workshop and to identify any gaps in understanding between what is being found in research and what is happening "on the ground" in the classrooms. The Alberta Teachers' Association is also a co-host of the event and there will be a number of educators among other interested observers attending.

Another project my office was involved in was last year's GPEN privacy sweep, which focused on apps and websites targeted at children and youth. This topic, as you may well imagine, received quite a bit of coverage as the sweep found that nearly half of websites and apps for children are sharing their personal information, but nearly 70% did not have effective controls to limit the collection of children's personal information[9]. The results of this sweep begged the

[8] http://www.equalityproject.ca/about/our-project/
[9] https://www.oipc.ab.ca/news-and-events/news-releases/2015/global-privacy-sweep-finds-half-of-websites,-apps-are-sharing-childrens-personal-information.aspx

question, “Why do organizations want to know this much about children and youth?”

In response to these results, my office collaborated with the Office of the Privacy Commissioner of Canada to develop a *Kids’ Privacy Sweep Lesson Plan* for students in Grades 7 and 8 to help develop their “digital citizenship” by becoming more aware of why their information is collected, understand what personal information is, and to help them to make informed decisions about the websites they visit and the apps they use[10].

Further, just last week at the International Conference of Data Protection and Privacy Commissioners in Morocco, a resolution was adopted on an “International Competency Framework on Privacy Education”, which places a priority on teaching children and youth on the protection of personal information for privacy regulators around the world[11].

I know this is a topic that many of you are involved in so I would appreciate any thoughts you may have that may advance the teaching of privacy in classrooms, and ultimately ensure students are communicating in safe and healthy online environments.

GDPR and the Privacy Law Landscape

The final topic I want to touch on today involves the European Union’s *General Data Protection Regulation*, or GDPR.

[10] https://www.oipc.ab.ca/media/604268/guide_kids_privacy_sweep_lesson_sep2015.pdf
[11] https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/an_161020_res/

Earlier this year, I submitted my recommendations to the Standing Committee on Alberta's Economic Future with regard to their review of PIPA, the private sector privacy law in Alberta[12].

In it, I stated that Albertans should be proud of PIPA but made a number of recommendations that sought to enhance the legislation in the context of developments in privacy law around the world, namely the European Union's *General Data Protection Regulation*.

As I said in my presentation to the Committee, PIPA was not created in a vacuum. There are global and national forces and principles that shaped how PIPA was drafted and how it must function to be recognized within Canada and by other nations.

The GDPR will officially come into force in May 2018 and will shift the privacy law and policy world. There are already some commentators questioning whether Canada's private sector privacy laws will maintain "adequacy" status once in force[13]. European law requires jurisdictions to have "adequacy" with regard to the protection of personal information to permit the cross-border flows of information.

As I stated earlier, the GDPR enhances protection of personal information and includes increased fines associated with contraventions of privacy law by businesses. The GDPR has enhanced the protections for Europeans' personal

[12] https://www.oipc.ab.ca/media/686362/PIPA_Review_Submission_Web_Feb2016.pdf
[13] http://www.privacyandcybersecuritylaw.com/impact-of-the-european-general-data-protection-regulation-gdpr-on-adequacy-and-5-tips-to-weather-the-changes

information in many areas, including around consent, accountability and privacy management frameworks, breach notification, and privacy impact assessments.

In some ways, we are ahead of the curve in Alberta with regard to mandatory breach reporting and notification provisions and, indeed, other jurisdictions in Canada and globally are attempting to catch up. But there are areas where we could do better.

The uncertainty of adequacy status with regard to the GDPR cannot be understated as the privacy world witnessed when the European Court of Justice struck down the Safe Harbor framework.

As you likely know, Safe Harbor had been the pact between the European Union and United States ensuring the protection of personal information flowing across international borders. For a variety of reasons, including information sharing revelations exposed by Edward Snowden, Safe Harbor was deemed inadequate.

This decision striking down safe harbor led to significant uncertainty and, as a result, increased costs for businesses trying to navigate the global economy without having a legal framework to ensure protections of personal information flowing across borders.

In light of this, while privacy laws and regulations may sometimes appear to be a burden, for organizations seeking to do business in a global economy, consistent, harmonized laws help to provide a stable framework to support business transactions and to reassure and protect consumers.

The recommendations I offered in my submission to the Standing Committee's review of PIPA recognized the global forces at play and made recommendations around transparency reporting and privacy management frameworks. Not to be a burden, but to both enhance the protection of personal information and to keep pace with developments in this area in the European Union, which sets the tone for the world in terms of privacy law.

Again, we are ahead of the curve in some respects with privacy management frameworks in Canada. In 2012, my office's work with the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia to publish *Getting Accountability Right with a Privacy Management Program* anticipated and is aligned with the new legal requirements in the GDPR around privacy management frameworks[14].

This document provides guidance to businesses for how they can manifest the principle of accountability within their own organizations. In harmony with legislative reform that is taking place in other jurisdictions, I recommended that the Committee reviewing PIPA consider legislating the requirements of a privacy management framework in the Act itself.

Just a quick anecdote that when our three Canadian jurisdictions released our *Getting Accountability Right* guidance, we received international accolades, including from the Chief Privacy Officer of a multinational corporation who called it the "gold standard" for the world to follow.

[14] https://www.oipc.ab.ca/media/383671/guide_getting_accountability_with_privacy_program_apr2012.pdf

PIPA is a strong piece of legislation that I believe requires some tweaks to ensure it remains a leader in private sector privacy law in Canada – and especially that we don't fall behind in view of the developments in other jurisdictions, particularly the EU.

At this time, however, it appears we will have to wait for those adjustments as the Standing Committee recently completed its report and has made only one recommendation for amendment: to clarify the definition of a commercial activity[15].

Conclusion

So, to wrap things up, I know my comments here today touch on just a few of the issues I'm sure you all are grappling with. New technologies and our interconnected world offer tremendous opportunities but also introduce many potential privacy risks.

The interplay between new technologies and privacy law is delicate. It requires constant review and revision of various protocols to keep pace as much as possible – and in the context of cybersecurity, keeping pace, if not a step ahead, is critical.

Thank you for the opportunity to be here today, and I'm happy to take any questions.

---

15 https://www.assembly.ab.ca/committees/PastReports/2016/Review%20of%20the%20Personal%20Information%20Protection%20Act%20Final%20Report.pdf