Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

UNDERSTANDING PIPA: BEST PRACTICES FOR SECURITY PROFESSIONALS

Elizabeth Denham
Information and Privacy Commissioner for B.C.

Speech to the
Vancouver Security Partners Forum
January 28, 2013

Good afternoon. It's great to be here and to see so many of you eager to learn more about private sector privacy.

I am going to begin by briefly describing my office and our role.

As Commissioner, my job is to enforce the *Freedom of Information and Protection of Privacy Act*, which covers the public sector—and the *Personal Information Protection Act*, which covers the private sector. We are "a small team with a big mandate". I have 32 staff overseeing the personal information practices of 2500 public bodies and 300,000 businesses and non-profits in B.C.

In addition to my investigative and enforcement powers, I have a mandate to make public comments on programs, policies and services affecting information and privacy rights in BC.

Some of the major files on my desk right now include: the review of the new BC Services Card, a review of the BC Government's Open Information and Open Data

portals, police information checks, the use of GPS in the workplace, and the use of Automated Licence Plate technology by municipal police.

Phew!

I also have a public education mandate. Not every regulator has one, but I do. I strongly believe that making citizens and organizations aware of their rights and responsibilities is essential to my work.

Speaking of public education… we are here on a very special day. January 28th is Data Privacy Day. Happy Data Privacy Day to you!! A day for regulators, businesses, privacy interest groups, and civil society groups around the world to promote online privacy, and highlight the impact of technology on privacy and personal information.

Here in B.C. last year we marked the day with a public education project about privacy and video surveillance in the retail sector. I'll say a bit more about surveillance later. And this year we are focusing on the value of privacy in the digital world—through focused outreach and speaking events like this one.

I was asked to use my time this afternoon to describe some of the key concepts, principles and practices you can use to promote privacy and security in your organization or business.

We're going to talk theory and practice. Because at the end of the day—it's about applying what you know about privacy to ensure the personal information of your customers, employees, and business partners is protected. I will also leave some time at the end for questions and answers. I look forward to having a conversation and hear about your challenges and solutions.

By a show of hands, how many of you knew before you showed up here today that B.C. has a private sector privacy law? This is one of the biggest challenges we face as a regulator. The *Personal Information Protection Act* ("PIPA") came into effect in January 2004—almost a decade ago! Yet I believe many businesses, especially SMEs. have little awareness of their legal responsibilities.

We are very much involved in informing businesses about PIPA—Because you can't get to compliance without first building awareness. In fact, after today you may find yourselves wearing this hat—advising your clients and prospective clients to make them aware of the rules governing personal information under PIPA.

But even businesses who have heard of PIPA can be a bit confused about the breadth of the law and what it covers. With that in mind, I'd like to review some frequently asked questions about the law, what it covers and what it doesn't. For those of you in the audience who are from the public sector and governed by the *Freedom of Information and Protection of Privacy Act* ("FIPPA")—please stick with me. There are a few nuggets in here for you, too.

- **WHO DOES PIPA APPLY TO?**

PIPA applies to the personal information practices of more than 300,000 organizations including not-for-profits, corporations, charities, small businesses… even political parties!

Some of you may do business in other jurisdictions across Canada. If so, you may be familiar with the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), the federal law governing private sector privacy.

B.C's law has been declared substantially similar to PIPEDA, and therefore the federal law does not apply to provincially regulated businesses. Alberta and Québec are the other provinces that have enacted private sector privacy laws.

BC's law has broader application than the federal rules for personal data in the private sector. This is because the federal law focuses exclusively on personal information processed for commercial purposes whereas our law applies to employee personal information and information held by non-profits.

Maybe an obvious point, but PIPA does not apply to citizens acting in their personal capacity. We can't investigate what your neighbour discloses about your lifestyle, nor what people post about their friends on social media.

- **WHAT IS PERSONAL INFORMATION?**

PIPA applies when an organization collects, uses or discloses personal information. But what does personal information mean? Here is the definition straight out of the legislation:

> ***"personal information"*** *means information about an identifiable individual and includes employee personal information but does not include contact information, or work product information.*

So, personal information means information that can identify an individual—for example, a person's name, home address, home phone number or ID number other than work contact information. It also means information about an identifiable individual—like a physical description, an image, or biometric, an identification number or blood type.

- **WHEN CAN I COLLECT, USE OR DISCLOSE PERSONAL INFORMATION?**

Before you can collect, use or disclose personal information you generally need consent from the person you are collecting it from. Consent must be at the front end of any transaction—to obtain consent, first you must notify an individual of your intention to collect, use or disclose their information and for what purpose. Once you have obtained consent, you can collect, use or disclose information for that stated purpose.

However, consent is not the silver bullet. Even with consent, PIPA only allows personal information to be collected, used or disclosed for a reasonable purpose.

OK, so what does reasonable mean? Under PIPA, reasonable means what a reasonable person would think is appropriate in the situation. In other words, what is reasonable will depend on factors such as the nature of your business, the kind or amount of personal information you collect, and how you plan to use or disclose that information.

The purpose has to have a nexus to the business transaction. For example, let's say you own a company that specializes in physical security and alarm systems. A customer walks through your front door and asks you to install a burglar alarm on his home. Clearly, you need to establish that the person is who they say they are… and that the home you are securing is actually theirs, before you do the work.

So, what personal information are you going to collect from this person? You might examine a driver's licence to confirm identity and proof of address. And, if you were setting up ongoing payments, maybe a credit card number or banking information for automatic debit.

But, let me ask you this: do you need to photocopy and retain the driver's licence data? Do you need to collect a social insurance number? What about gender, or birthday, or a list of individuals living in the home? These are all important questions to ask as you consider what is necessary to collect for the purposes of doing business, and what is not?

My final point in this section—it is against the rules of PIPA to use personal information for a different purpose than for which you collected it. We call this "function creep". For instance, if your customers consented to give their name, home address and postal code for the purposes of warranty protection on the alarm system you installed, you cannot turn around and use that information for target marketing. You cannot use that information to email them special offers or mail them flyers. You cannot share it with third parties for research into which neighborhoods are most likely to buy similar products.

- **WHAT ABOUT INVESTIGATIONS AND SURVEILLANCE?**

I include this section for all of the private investigators in the room today…Since much of the work you do relates to collecting information from individuals without consent. Organizations might hire you to conduct investigations or covert surveillance on their behalf.

Let me be clear—while the legal responsibility to comply with PIPA ultimately rests with the client organization, I believe that there is a shared responsibility to ensure that the collection, use and disclosure of personal information is done in accordance with privacy laws.

Under PIPA, there are very limited and specific circumstances in which you can collect personal information without consent.

First, if collection with the knowledge and consent of the individual would compromise the availability or accuracy of the information.

Second, if the collection is for purposes related to investigating a breach of an agreement or a contravention of the law.

Or—if the collection is authorized by law.

Unless your activities fall into one of these categories, then you must get consent before proceeding.

Finally, even **if** you have the legal authority to proceed with covert surveillance, there are a number of factors you must satisfy before you have the authority to collect images, recordings and other information.

Privacy Commissioners federally and provincially have found that covert surveillance is highly intrusive; therefore businesses must step very carefully:

- Is the collection for a legitimate business purpose?
- What information is reasonable to collect in the circumstances? Ensure you are not collecting information about individuals that are not the subject of the investigation.
- Are there other less privacy-intrusive means to collect the information other than covert surveillance? For example, can you require a third party medical assessment for the investigation of a disability claim?

Sidebar: It's a common misconception that an organization is relieved of its privacy responsibilities when a person is in a public place! Expectations of privacy may be diminished, but businesses are still required to limit what they collect and collect data only for reasonable purposes.

PIPA seeks to strike a balance between the legitimate needs of business, and the inherent privacy rights of the individual. There has to be a balance between security and privacy rights.

- **WHAT IS "REASONABLE SECURITY"?**

This last question is a popular one.

We have already talked about the conditions under which you can collect, use and disclose information under PIPA. You also have a legal requirement protect and secure personal information in your custody. In other words, you are accountable for the handling of that data. You must have the appropriate administrative, physical

and technical safeguards in place to protect personal information against risks like unauthorized access, theft, accidental disclosure or improper disposal. We call this "reasonable security" and it is a requirement in both the public and private sector legislation.

But "reasonable security" is not a one-size-fits-all standard. Because situations vary, the measures needed to protect personal information will vary.

As a regulator, we assess compliance with "reasonable security":

- in response to a privacy breach;
- in the course of investigating a complaint; and
- in a Commissioner-initiated investigation or audit.

Let me give you just two quick examples—this time from the public sector—about how reasonable security is measured in practice through our enforcement work.

In January 2012, thieves broke into the Administrative Services Building at the University of Victoria. One of the items stolen was a USB flash drive containing the names, SIN numbers and banking information of 12,000 current and former employees.

UVic reported the breach to my Office, and I decided to launch a comprehensive investigation given the severity of the breach and the number of individuals affected. We examined the University's compliance with "reasonable security" arrangements – a requirement in the law.

What we found was that the University was aware of its obligation to safeguard sensitive personal information using a range of protective measures. They had sound fundamentals of data governance: they appointed a privacy officer, approved a privacy policy, and had completed training workshops to raise awareness about privacy and security at the University. All very important stuff. However, there was no clear policy, or direction to establish a sufficiently high standard for protecting the type of information stored on mobile devices like laptops and USB keys. A critical area of vulnerability in all organizations.

Given the method of storage—a portable device—and the sensitive and confidential nature of the information—we determined that encryption—not just password protection—is the minimum security standard. Because UVic had failed to implement this level of protection, they failed to meet the "reasonable security" test under section 30 of FIPPA. The breach response and the aftermath cleanup ended up costing the university hundreds of thousands of dollars.

This next example will be familiar to the folks from the BC Lottery Corporation who are in the room today.

On July 16 2010, BCLC launched a new online gaming platform called PlayNow.com. On the date of launch, because of a software glitch, sensitive customer details, including names, bank account and credit card numbers, were displayed to other PlayNow customers.

My office initiated a two-part investigation. First, we assessed the privacy breach that occurred on the 16th of July.

Second, we launched a second, more detailed investigation that examined the general security of the PlayNow platform. This was the first time my office had ever investigated an online platform, and addressed the unique security considerations of online services. Online platforms have privacy and security risks that are not common to other systems such as phishing, malware and spyware. Government's involvement with gaming requires an increased level of trust and confidence on the part of customers. With this increased level of trust comes an increased level of responsibility.

Finally, given the circumstances, I found that online systems require proactive and ongoing monitoring, testing and training to ensure policies, procedures and systems are up to date. After examining the security of the online platform, we found that BC Lotteries failed to have reasonable security arrangements in place when PlayNow was first launched.

The individual deficiencies uncovered by our investigation—including user access and malicious code controls, inadequate processes for system patches, and some unencrypted data transmissions—may not on their own trigger a failure in the "reasonable standard" test.

But taken cumulatively, we found that there was not a reasonable level of security in place when PlayNow went live. The site was down for nearly five weeks while BC Lotteries addressed the deficiencies—at their estimated cost of $150,000 dollars a day in lost revenues. And to their credit—since this incident, BCLC has implemented strong data governance across the organization.

I was recently on a site visit to BCLC, and we were heartened by the corporate-wide efforts to implement a culture of privacy throughout the corporation.

These examples show that "reasonable security" is not a one-size-fits-all standard. The key to compliance is a thorough assessment of your own operating environment. Careful consideration of the different factors at play—including risk, technology, and the type and sensitivity of personal information collected—is critical. As is ongoing evaluation to ensure those processes are being followed.

Some of you might be out there thinking, OK. I get it. Privacy laws apply to my business. But why should I care? What is the incentive to comply?

First, know that privacy matters very deeply to your customers. A study released last month by MacLaren McCann shows that nearly three-quarters of Canadians are worried about the erosion of their personal privacy. Canadians' fears about privacy

are second only to worries about the global financial crisis, and have surpassed climate change and terrorism.

If you have strong privacy practices, and you know your clients and customers are very live to these issues—it can be an asset in terms of your marketing and setting you apart from your competitors. So, protecting privacy is not just the right thing to do from a legal compliance perspective—it can also create a competitive advantage for your business.

Second, I would suggest that given the nature of the services you provide, there is an expectation in the minds of consumers that you take privacy seriously. Many of you are in the security business. Your existing customers might expect that you take an equally serious approach to protecting their personal information as you do to securing their physical property.

I would also suggest that there is an **expectation** that you would have a more sophisticated understanding, perhaps more so than in other sectors—of your responsibilities under PIPA, what is at stake, and that you will have implemented secure systems for storing and protecting your clients' personal information. In other words, your customers may hold you to a higher standard. All the more reason to figure this privacy stuff out, right?

So how do you take some of the principles we've talked about – and translate them into privacy-positive practices for your business? I know it sounds overwhelming… but we have a toolkit that can help you.

In 2012, Canada's Commissioners responsible for private sector privacy got together to publish "Getting Accountability Right with a Privacy Management Program."

It is a building-block framework that will help you implement a privacy management program—a model that you can apply across your organization—to ensure that every aspect of your business respects privacy laws. By implementing these building blocks, you can demonstrate to your customers, employees, and regulators that you are committed to privacy and accountability, enhancing your reputation and building trust in those relationships.

The building blocks begin with corporate organizational commitment to develop a privacy-respectful culture. This has to start from the very top – with buy-in from senior management. Only then, can responsibility be truly delegated to a Privacy Lead, perhaps supported by a team with delegation and clear roles and responsibilities.

Next are the program controls, starting with an inventory of what personal information you hold, where it is held, its level of sensitivity and the purposes for which it is being collected, used and disclosed. Once the building blocks are established, you need to have a mechanism in place to monitor, assess and improve your program.

The bottom line: Privacy management is not a one-time thing, or a one-off. You can't say, privacy, yeah, we took care of that in 2004. It takes a fundamental commitment, supported by a strong team and a commitment to a culture of privacy. An investment in privacy and security up front is a far better bet than cleaning up the mess after a catastrophic data breach, which could be as simple as a lost USB key—a costly way to erode public trust.

And let me say that it's not just smaller businesses that need some guidance on this stuff. Big corporations can get this stuff wrong, too.

You might remember the storm of controversy surrounding Google, when it was revealed that their fleet of cars collecting data for Street view were found to be vacuuming up unsecured WiFi data without notice or consent. A practice that cost Google huge sums in the wake of dozens of regulatory investigations.

Perhaps the most revealing thing about the Google case was the fact that the engineers designed the system to collect this data without the knowledge of some of the key players in Google, including those responsible for compliance with privacy and consumer protection laws. What they were lacking was a foundation of data governance that went across the organization.

So, nobody's perfect. Not even internet giants like Google. And the best part is that you can begin to take steps today to implement a foundation of accountability for your business, build a culture of privacy and avoid these costly pitfalls.

First things first:

- Build a culture of accountability along with other key decision makers in your organization.
- Designate a privacy officer. Support their work across the company to build a robust privacy framework.
- Once you have a privacy lead – and you may be the person wearing this hat! Make sure you are at the table when decisions about new products, services and business models are made.
- Document what personal information you hold, where it is held and the level of sensitivity. Is it in the hands of service providers? You are still legally accountable for this data at the end of the day.
- Create contingency plans in the case of a privacy breach. You will need a command and control approach to properly manage a breach. Best to be clear ahead of time what roles you will play and who is calling the shots.
- I would also encourage you to do some spot audits to test how well your policies are being implemented.

These are just a few examples of how the accountability tool can be made to work for you.

The tool is available for download on our website. I have brought some paper copies with me – come see me after the presentation and I would be happy to provide one.

Thank you for your attention this morning.

Visit our website to download the accountability tool. We are also on Twitter—you can follow us at BCInfoPrivacy.

I'm happy to take some questions from the floor.