CHECK AGAINST DELIVERY

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Privacy: What You Need to Know

Elizabeth Denham
Information and Privacy Commissioner for B.C.

Keynote Presentation to the Professional Investigator's Association Conference
Victoria, BC
October 26, 2013

Thank you very much.

I like to open my speeches with a little bit of humour, but then I started to think about how many Magnum PI jokes you probably hear at these events so I think I'll stick to the facts this time.

It's a pleasure to be here. Earlier this summer I met with Taras, Dale, Dave Jones and Greg Tweed to talk about your profession and some of the issues you're facing. They also told me about this conference, focused on the future of professional investigation.

By way of coincidence, we just wrapped up our own forward-looking conference, held in celebration of the 20th anniversary of the *Freedom of Information and Protection of Privacy Act*, which is our public sector law. We spent two days in Vancouver, celebrating the past but also looking to the future, and the challenges of protecting privacy in the internet age.

I'm happy to share some of my thoughts about the future of privacy enforcement with you today.

OVERVIEW

I'd like to start with an overview of BC's private sector legislation—I find that this is the area where there is a gap in knowledge about the law and how it applies. I also suspect this is the law that most of you are governed by. Some of you may have some public sector exposure but I'll deal with that later. Then I'd like to turn to the future of privacy law in BC from a regulator's perspective.

A few words about my office and mandate: 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. There are 32 staff, including investigators, lawyers, policy analysts, and our intake team, doing this important work.

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 before my office recently include:

- Review of Phase 1 of BC Services card
- Use of Facial Recognition Technology by ICBC
- Use of Automated Licence Plate Recognition by Victoria Police Department

I also have an important public education mandate. I strongly believe that making citizens AND organizations aware of their rights and responsibilities is essential to my work. Educating the private sector is one of the biggest challenges I face as a regulator. Many businesses, especially small, have little awareness of their legal responsibilities under the private sector law.

My office recognizes this, and we are very much involved in educating these businesses about PIPA because you can't get to compliance without first building awareness. But even businesses who have heard of PIPA can be a bit confused about the breadth of the law and what it covers. Some of you may be in this boat.

With that in mind, I'd like to review some common questions we get about the law, what it covers and what it doesn't.

WHO DOES PIPA APPLY TO?

PIPA applies to 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 PIPEDA—the federal law governing private sector privacy. BC's law has been declared substantially similar to PIPEDA, and therefore the federal law does not apply within BC's borders.

Interestingly, our 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 fully covers employee personal information and information held by non-profits.

PIPA does not apply to citizens acting in their personal capacity. So it doesn't apply to individuals taking photos or videos of others. It doesn't apply to the posts you make of your friends online or the compilation of your Christmas card list.

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, their images, their voice print or an ID number, even an IP address in certain contexts, other than work contact information.

COLLECT, USE, DISCLOSE

Under PIPA before you can collect, use or disclose personal information you must obtain consent from the person you are collecting it from—with a few exceptions. 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. But, consent is not the silver bullet.

Even with consent, PIPA only allows personal information to be collected, or disclosed for a reasonable purpose. 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. 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 an alarm system for their 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 look at a driver's licence to confirm identity. You might also ask for a proof of address. And if you were setting up ongoing payments, maybe a credit card number or cheque.

But, let me ask you this: do you need to write that driver's licence number down? Do you need to collect a social insurance number? What about a phone number, gender, or birthday? These are all important questions to ask as you consider… what is reasonable 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 new or different purpose than for which you collected it. We call this "function creep."

For instance, if your customers consented to give their name, 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 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 what neighborhoods are most likely to buy similar products.

INVESTIGATIONS AND SURVEILLANCE

Much of the work you do relates to collecting information from individuals without consent. Organizations might hire you to conduct 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 c**onsent. First, if collection with 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.

Unless your activities fall into either of these two categories, then you must get consent before proceeding. That is what the law says.

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:

- 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 workplace claim?

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

I hope these PIPA basics to give you a frame of reference for your business. BTW, there are guidance documents for both overt video surveillance and covert surveillance on our website and the website of the OPC.

I'd now like to turn now to the future of privacy enforcement in British Columbia.

As a regulator, I am changing our approach—and it will directly impact how you conduct your business in terms of compliance with the Act and also liaising with your customers and clients.

ACCOUNTABILITY

The name of the game is “Accountability.” Accountability is a core principle of our privacy laws. It is one of the 10 privacy principles laid out in the federal law, PIPEDA, and it is fundamental to our provincial laws.

Accountability basically means, any organization that collects, uses or discloses personal information in the course of doing business, is legally and ethically accountable for the security and management of that information from start to finish.

How does one achieve accountability? By implementing a comprehensive privacy management program—so that all information systems, paper or electronic, embody the same core privacy principles—minimizing risk for data spills and accidents, but also providing evidence in the wake of an investigation that you are doing your due diligence to protect personal information in your care.

One of the major reasons for this shift to accountability is that many businesses say that protecting privacy is important, yet they fail to implement the necessary measures to create a culture of privacy.

Even after a decade under PIPEDA and PIPA, many do not have policies, practices, training or audit mechanisms in place to assess how, or how well personal data is protected. We have published detailed guidance to give private sector companies a roadmap to success. Jointly authored by three privacy regulators, it is your blueprint to privacy management. With this document also comes a shift in expectations among Commissioners in terms of enforcement and audit activities. Instead of focusing exclusively on reactive investigations and audits—for example, in response to a complaint or a story in the news—we are becoming more proactive in addressing privacy and security issues. And with the accountability framework, we've put organizations on notice that we expect to see evidence of a privacy management framework in place as part of our enforcement work. This shift to accountability is important for you in two ways.

First, it raises the bar for managing privacy within your company. If our investigators come knocking, we will expect to see evidence of due diligence and your privacy management program. We want to see policies, training and actions that breathe life into the legal requirements. It will be part of our assessment of your compliance with the law.

Second, it marks a raising of the bar on the part of your clients to properly manage personal information. This is going to become increasingly important for those of you who contract with the public sector in BC.

Our office has provided specific accountability guidance for public bodies like ICBC and WorkSafe BC, and made it clear that we expect to see privacy management adopted across these organizations—which we will be asking for them to demonstrate when we look under the hood.

Those of you who are contractors with these public bodies—will see that privacy management will also trickle down to you. Some of you might be thinking, jeez, this is going to create a lot of extra work for me, consider it this way. If you implement privacy management, and can readily demonstrate your policies, processes and safe guards, you will have a tremendous competitive advantage as you seek out contracts, particularly with the public sector.

And the good news 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 costly privacy pitfalls.

First things first.

- Designate a privacy officer. Support their work across the company to build a robust privacy and security 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.
- If you don't already have one, implement a privacy policy. You are required to have one under PIPA.
- 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 accountability can be made to work for you, and give you a competitive advantage in your business. The guidance document is available for download on our website.

In closing, privacy compliance and a high standard of safeguarding of personal information in investigations is critical to maintain and enhance public trust in your work.

I'm happy to take some questions.