Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

ADDRESS TO THE

PROFESSIONAL INVESTIGATORS ASSOCIATION OF BC

OCTOBER 22, 2016

DREW MCARTHUR
ACTING INFORMATION AND PRIVACY COMMISSIONER FOR B.C.

Good morning. Thanks to Taras for inviting me to speak to you today.

It's great to be here and to know that so many of you are eager to learn more about B.C.'s private sector privacy legislation.

I say "more" because the OIPC – that is, the Office of the Information and Privacy Commissioner – has spoken to your organization before.

By a show of hands, how many people in this audience would say that you're confident in your knowledge about B.C.'s *Personal Information Protection Act*, aka "PIPA."

OK, that's pretty good!

I have to tell you, awareness of privacy obligations is one of the biggest challenges we face as a regulator, with both private AND the public organizations.

PIPA came into effect in January 2004—more than a decade ago! My office has done a **lot** of public education since then. Yet many businesses still have little awareness of their legal responsibilities under the legislation.

(None of you in this room, of course.)

But just in case, I'll begin this morning by sharing some of my thoughts on how PIPA affects you as a professional investigator – what you need to know, what you need to do, and why, as professional investigators, you should do it.

Bear Mountain was recently the site of a PGA Tour Champions event, so without further ado, let's tee it up….

First – a bit about me. I was sworn in as Acting Information and Privacy Commissioner on July 6. This is a temporary assignment to fill the vacancy left by former Commissioner Elizabeth Denham, who spoke with you back in 2013. She completed her term at the OIPC and has now taken on the role of Information Commissioner for the U.K.

A new commissioner must be appointed by a **unanimous recommendation by an all-party committee** within 20 sitting days, when the Legislature is in session again.

I expect this will be in the spring.

In my previous life, I was "**the Privacy Guy**" from TELUS. I spent most of my career there and at the former BC TEL, where we were subject to several different legislative regimes.

I've been a member of the OIPC's External Advisory Board for the past six years, Now, I have been given a unique opportunity to see privacy and access to information through the lens of a regulator.

And… even though I will not be the permanent commissioner, I plan to use my time productively.

As Acting Commissioner, my job is to enforce PIPA as well as the *Freedom of Information and Protection of Privacy Act*, or FIPPA.

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.

I also have a public education mandate. Making citizens and organizations aware of their rights and responsibilities is essential to my work, which is why I'm here today.

I was asked to speak a bit about your line of work and the value of an organization like the Professional Investigators Association of B.C.

Unlike the fictional Jim Rockford -- who printed business cards in his car -- **you're** here today because you care about professional ethics and values.

Your organization has a comprehensive privacy policy, you follow a prescribed code of ethics and professional conduct… as members, you are all mandated to take an online professional private investigation training course, which our office reviewed…

you are licenced by the BC government's Security Programs Division…. All of that is great.

And… correct me if I'm wrong… you're listening to me right now, instead of catching an extra hour of sleep or maybe a bit of golf, because you care about privacy management and compliance with B.C.'s private sector privacy legislation. Again - great.

But even professionals like you who are familiar with PIPA and FIPPA can sometimes be confused about their breadth.

With that in mind, I'd like to review a few facts about the law. I'll give you some information about possible legislative changes… and I'll tell you a few simple things you can do to increase your privacy awareness quotient.

First of all, PIPA applies to the personal information practices of more than 380,000 organizations, including not-for-profits, corporations, charities, small businesses… even political parties!

FIPPA applies to over 2,900 public bodies in B.C. I'm assuming that some of you here today have worked for ICBC or another public body; when you are working in that capacity, it's the rules of FIPPA you must follow.

For instance, FIPPA comes into play with the collection, storage, and use of personal information from any ICBC surveillance, interviews, or skip tracing you may have been hired to conduct.

As some of you may do business in other jurisdictions across Canada, you also need to 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, so the federal law does not apply to provincially regulated businesses. Alberta and Québec are the other provinces that have enacted substantially similar private sector privacy laws.

The federal law focuses exclusively on personal information processed for commercial purpose, while our law applies to personal information held by any private sector organization, including not-for-profits.

PIPA applies when an organization – like a private investigation firm – collects, uses, or discloses personal information.

What is personal information? It is any information that can be linked to an identifiable individual, either on its own or in combination with other readily available information. That sounds broad because it is… and for good reason.

In other words, personal information is information that can identify an individual—for example, a person's name, home address, home phone number or ID number. And

information about that individual—like a physical description, an image, or biometric, an identification number or blood type.

Personal information is obviously **critical** to the work you do as investigators. But under B.C.'s privacy legislation, there are some important rules you must observe.

One of the most important issues – and most complex – is **consent**.

Much of the work you do as investigators involves collecting information about individuals without consent.

But you cannot inherit the collection rights of your client, so for example, while your client may be authorized to collect the personal information of an employee without consent, you do not have that authority.

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

You can collect information without consent while investigating a breach of an agreement or contravention of the law IF obtaining knowledge and consent of the individual would compromise the availability or accuracy of the information.

So, unless your activities meet this standard, then you must get consent before proceeding.

However, even when authorized, PIPA only allows personal information to be collected, used, or disclosed where a reasonable person would consider it appropriate.

What is reasonable will depend on factors such as the nature of your business, the kind or amount of personal information you need to collect, and how you plan to use or disclose that information.

I'll give you an example from two Orders my office issued about the use of GPS devices to track employees who were working remotely.

These Orders – for Schindler (an elevator supply company) and the University of British Columbia – are a few years old, but they offer important lessons.

In both cases, the employers combined location information from a GPS with devices that monitor distance, speed, acceleration, deceleration, idling time, and time of day when the vehicle is turned on and off.

Both Schindler and UBC argued that the information collected and used by the systems was about the **vehicles**, and not about the employees who drove them.

They argued that they could do whatever they wanted with the systems because they did not involve the use of personal information. My predecessor disagreed.

After a careful analysis, she had little doubt that the data collected and used by the vehicle monitoring systems was, in fact, personal information about the employees who drove those vehicles.

Schindler demonstrated that it was using the system to manage productivity, map routes, and manage hours of work—all of which we found to be legitimate, reasonable business purposes.

So, Commissioner Denham concluded that the information collected and used through Schindler's telematics system was "REASONABLY required to manage the employment relationship."

Similarly, she found that UBC's purpose for using vehicle monitoring for its campus security staff were necessary to ensure the safety of the employees, who often work on their own, and was therefore compliant with FIPPA.

In both cases, we were satisfied that managers were **not** engaged in continuous, real-time surveillance of employees, which would have been considered UNREASONABLE. The line between this legitimate use and continuous, real-time surveillance may seem like a fine one, but it is critically important, especially today.

As all of you know, the market is flooded with surveillance devices, from high-end professional units to covert video cameras disguised as smoke detectors, clock radios, even bird houses (!).

Some of these devices sound like they are straight out of a James Bond movie.

But before you deploy one of these devices, you should know that Privacy Commissioners federally and provincially find covert surveillance to be highly intrusive.

Ask yourself:

- Is the collection for a legitimate business purpose?
- What information is reasonable to collect in the circumstances? For instance, you must ensure you are not collecting information about individuals that are not the subject of your investigation.
- Are there other less privacy-intrusive means to collect the information other than surveillance?

You also have a legal requirement to 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 unauthorized access, theft, accidental disclosure or improper disposal.

We call this “reasonable security measures” and it is a requirement in both the public and private sector legislation.

This is important for you due to a change that is coming in our federal privacy legislation: **mandatory breach notification**.

Currently, Alberta is the only province in Canada to have mandatory data breach reporting requirements for all private sector organizations.

In 2015, the federal *Digital Privacy Act* received Royal assent in Canada’s Parliament. It amended PIPEDA to require private sector organizations to notify Canadians when they are put at risk as a result of their personal information being lost or stolen. This new notification requirement will come into force when the federal government issues its breach reporting regulation, likely within the next year or so.

As I mentioned earlier, B.C.’s PIPA has been deemed “substantially similar” to PIPEDA, and must remain so, meaning any legislative changes on the federal level must also be introduced here in B.C.

How could this change affect your business? Let me paint a picture.

Imagine you recorded several hours of video surveillance in Kamloops and are travelling home to your office in Vancouver. En route, someone breaks into your trunk and steals your video camera. Think of it - under an amended PIPA, and potentially, FIPPA, you could be required to notify **all** the people in your video about this as well as my office. If that video was covertly collected you could find yourself in a pretty awkward situation!

The key to preserving your reputation AND complying with privacy legislation involves making an honest assessment of your operating environment. How secure are your practices?

Carefully consider the factors at play—risks, technologies, and the type and sensitivity of personal information you typically collect.

Develop security protocols and evaluate your practices regularly to ensure they are being observed.

Given the nature of the services you provide, there is an expectation that you take privacy very seriously – more seriously, in fact, than other organizations.

Adopting privacy-positive practices can create a competitive advantage for your business.

I know it sounds like a lot of work – but we have a toolkit to help you.

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

This building-block framework will help you implement a privacy management program to ensure that your business respects privacy laws.

You'll be able to demonstrate to your customers, employees – and the regulators – that you are committed to privacy and accountability.

Begin with a commitment to develop a privacy-respectful culture. Then responsibility can be delegated to a Privacy Lead, which may be you.

Next come the program controls. Take an inventory of the personal information you hold, where it's held, its level of sensitivity, and the purposes for which it is being collected, used, and disclosed.

Once these building blocks are established, you'll need to have a mechanism in place to monitor, assess, and improve your program.

The bottom line: Privacy management requires regular care and feeding.

But investing in privacy and security is far better than cleaning up the mess after, say, the theft of that hypothetical video camera.

Once you've developed and implemented a privacy management plan, we have tools on our website to help you create a detailed **privacy policy** for your website.

Letting your clients – and potential clients – see everything you're doing to protect their privacy and adhere to B.C.'s privacy legislation will speak volumes for your integrity, professionalism, experience, and confidentiality.

Thank you for your attention this morning.

I hope through this talk I've increased your privacy awareness quotient.

Please feel free to contact my office any time for more information.