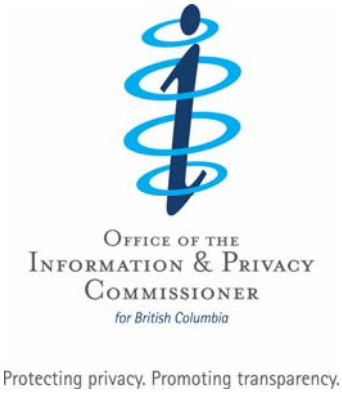

CHECK AGAINST DELIVERY

PRESENTATION TO

DESTINATION BC

JANUARY 25, 2017

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

Good morning, everyone. It's great to be here with the folks behind the Super, Natural British Columbia brand. Thanks to **Kate** for inviting me to speak with you today.

These sorts of gatherings offer a chance to socialize with colleagues from other departments…. To learn…. And to collaborate with one another as you work on common corporate goals. I hope it's been a great day for you so far.

I understand the key themes of your meeting are aspirational… "Courage, social media, innovation, and digital strategy." These are themes that, incidentally, also impact our daily work at the Office of the Information and Privacy Commissioner, as I will explain.

But before I get too far into my presentation, I'd like to tell you that the Information and Privacy Commissioner role is a temporary assignment for me. I was sworn in on July 7, at the end of my predecessor's term.

According to our legislation, a new commissioner must be appointed by a **unanimous recommendation by an all-party committee** within 20 sitting days, when the Legislature sits again on February 14.

So I guess you could say that you've taken advantage of a special, limited-time offer by inviting me here to speak with you today.

I actually spent most of my career at TELUS and the former BC TEL, where I was known as “the Privacy Guy.” That was MY brand. I also managed my own consulting company and served on the former commissioner’s external advisory board. Now I’m responsible for enforcing B.C.’s privacy and access to information legislation. From the **regulated** to the **regulator**… it’s been quite an eye opener.

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 of British Columbians.

I also have a public education mandate. Making citizens and organizations aware of their rights and responsibilities is essential to my work, and that’s one of the reasons why I’m here today.

Specifically, I’d like to talk to you about how privacy affects the work you do at Destination BC. Please don’t be afraid to speak up if you’re curious about any aspect of our work.

It is my understanding that Destination BC is a **very** media-savvy organization, and that a lot of the promotion and discussion around travel opportunities occurs online. In preparing for this speech, I checked out your “Wild Within” video on YouTube. I have lived here all my life, and want to compliment you on how well you’ve captured the magic of B.C. It made me yearn to be out on my boat… crossing the Salish Sea to the Gulf Islands… enjoying some of the world’s greatest cruising.

Wherever else they venture, those who visit B.C. establish very close bonds to our province. As marketers, you want to tell their stories… you want to share their personal experiences… you want to **inspire** others to come to B.C as well.

In our digital age, “sharing” of course involves tools like social media, user-generated content, live streaming videos, digital photography, and e-marketing – areas where privacy concerns can come into play.

Let’s take a closer look at some of these concerns.

First of all, Destination BC holds a somewhat unique position. As a Crown corporation, you are a public body. But you share a mandate and you work very closely with **private** organizations.

This means that **both** of our privacy laws – the public sector *Freedom of Information and Protection of Privacy Act* and the private sector *Personal Information Protection Act* – impact tourism. I feel your pain: at TELUS we were subject to several different legislative regimes.

It can be confusing, no doubt. But I think I can simplify things for you, whether you’re flying a drone with a video camera attached or simply posting a tweet. Just know this: The principles are the same for both pieces of legislation.

As a public body, you will **always** be bound by FIPPA – the *Freedom of Information and Protection of Privacy Act*.

Any volunteer or service provider to your organization is also bound by FIPPA, as they are considered "employees" of Destination BC.

How do you know when a business is a service provider? FIPPA states that a service provider is a "person," which includes an organization, retained under a contract to perform a service for a public body. That's pretty simple.

So, to give you an example, the videographers you hired to create that amazing video are bound by FIPPA when they work for you and you are also responsible for how THEY handle personal information.

Other industry players, like ski resorts, attractions, or tourism operators… any of your stakeholders who are not public bodies… fall under PIPA, the private sector legislation. And so does that videographer, when he is not working on contract for you or another public body.

Are you still with me?

PIPA is **consent-based** and governs the collection, use and disclosure of personal information by organizations. It recognizes the right of individuals to protect their personal information **as well as** the need of organizations to collect, use or disclose personal information for business purposes, as long as those purposes are appropriate under the circumstances.

It would frustrate commerce, for instance, if we said that a bank couldn't collect personal information from you when you go in to open a chequing account.

Does everyone here know what I mean by personal information?

Contact information used for the purpose of finding someone at their place of business is not restricted by the Act. Let's say, for example, you want to include the business information at the end of a blog about a winery in Kelowna. This is not personal information.

So what ***is*** personal information then? Well, if it's about you, and it's not business contact information, it's personal information. Here are a few examples: your age, marital status, blood type… your race, nationality, ethnicity… your salary information, social insurance number, health ID, PIN numbers… and any photos and videos of you…. These are also personal information.

And, in our brave new world, biometrics – the measurement of your unique physical characteristics, like fingerprints, iris scans, and your facial features… these are also very much personal information. They're unique to us. And they can definitely identify us.

However if a person is not identifiable, the Act does not apply. Here's an example: I saw a picture of someone mountain biking in the snow on your Twitter feed. He was wearing an oversized jacket, helmet, and goggles. I think it is safe to say that this person is not identifiable – so our privacy legislation would not apply to this image. Our privacy law would only take effect if you added more information, such as maybe the date, that would make it more likely that the mountain biker could be identified.

If so, you can still use this person's personal information, but you need to know what rules apply…what you can and cannot do with it.

Consent has been one of the cornerstones of privacy since the early 1970s – around the time B.C.'s Hotel Room Tax was introduced, and just before construction began on Whistler Village, one of my favourite getaways.

Consent is important because it allows people to decide how their personal information is collected, used and disclosed by governments and organizations.

GoPros, for example, offer an interesting privacy challenge, as they can indiscriminately capture the personal information of others without their consent, on ski hills, river rafts, and beaches… anywhere and everywhere we "go."

As you may know, the Act was updated a number of years ago to address the issue of social media and public events. Section 33.1(1)(q) of the Act says that a public body can disclose PI inside or outside of Canada if the information was collected by observation at a presentation, ceremony, performance, sports meet or similar event.

This means that you can post images taken at public events, like this weekend's Chinese New Year parade. But…this only applies if the event was open to the public and the individuals attended voluntarily.

So if you are live streaming at an event, or interviewing someone at a music festival, you can disclose the images of the people captured the background. But this rule doesn't apply to a typical public situation, like filming a group of early morning walkers at Stanley Park.

What about all those engaged and enthusiastic travellers posting comments on your Hello BC blog? Or when you retweet the Explore BC hashtag on your Destination BC Twitter account? This counts as a disclosure by a public body because you, the public body, facilitate that disclosure.

Speaking of live streaming, I'd like to spend a minute on video surveillance. My office recently completed an audit of a medical clinic in the Lower Mainland that was over-collecting personal information of staff and clients without consent and without authorization via security cameras. Any tourism operators who use video surveillance should only do so as a last resort and ensure they have proper signage in place to notify people.

Mobile apps, too, can be an area of concern, as we discovered during a sweep we conducted in 2014 with 26 other privacy regulators from around the globe.

Our B.C. Office examined 15 apps for Apple and Android platforms with a focus on the financial sector. We found that a majority of the apps failed to provide information about privacy practices as required by B.C.'s privacy law. PIPA requires notice and consent from an individual before collecting, using or sharing personal information. Yet 54% of the surveyed apps did not meet this standard.

App developers must provide clear information to users about how personal information will be collected, used, and disclosed. This information should be available up-front, before an app is downloaded, and should also be included in a privacy policy posted to the web. In other words, privacy needs to be part of the design of any mobile app.

Did any of you see the recent episode of Marketplace called "Are your apps spying on you?" If not, I recommend that you watch it on CBC.ca. This show underscored just how much our privacy can be compromised when we download a seemingly harmless mobile app.

As a side-note, in your marketing programs, be especially wary of organizations that offer to provide you with a so-called "consent-based list," especially those based outside Canada. You may be in contravention of Canada's anti-spam legislation.

So – what's the bottom line here? You need to follow the rules of FIPPA when you collect, use, and disclose personal information. Most public bodies can collect personal information if it relates directly to and is necessary for a program or activity of that public body. I'm sure most of you already know this. You can use personal information for the purposes for which you collected it, BUT you need to get consent to use it for a different purpose.

FIPPA also has rules about keeping personal information accurate and complete, keeping it secure, and for how long you can retain it. For instance, how long should you keep resumes after a job competition, or contest ballots, once you've announced a winner…

These rules apply to how your organization handles the personal information of citizens and visitors. They also apply to you, as the employees and directors of a public body. As an organization, you have an obligation to protect the privacy of your staff. Employees, as we say, do not check their personal privacy at the door to the office.

We encourage both public and private organizations to develop privacy policies and take the time to train staff. And if you know you're going to be running a contest as a part of your campaign, for instance, include a line in your project plan for a privacy impact assessment. It doesn't have to be complicated and we have many helpful guidance documents on our website.

You may be wondering at this point – does privacy even resonate in our digital age? When former Google CEO Eric Schmidt was asked whether users should be concerned about sharing so much information with Google, he responded, “If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.”

It won’t surprise you to hear that I disagree – intensely – with Mr. Schmidt’s suggestion. I very much believe privacy is an essential democratic right and worthy of protection.

I also believe privacy is alive and well, and that the public is more aware and more concerned about their privacy rights today than ever before. According to our constitution, even criminals have privacy rights. Canada has a well-established network of privacy regulators, both provincially as well as at the federal level. Back in 2009, the then Privacy Commissioner of Canada was the first regulator to look at social networking sites like Facebook. Their report brought privacy risks and necessary fixes to light, and prompted significant changes in how Facebook handles the sensitive personal information of its Canadian users. You really **can** take on the giants.

The report also generated awareness with the public of what they were potentially losing. As a result both consumers and regulators around the world continue to closely monitor Facebook and other social media sites.

Travellers to B.C. are of course part of that educated public. Many are well aware of their privacy rights and they count on public and private organizations in B.C.’s tourism industry to protect them. When you as leaders in your industry do so, you instil confidence, you build trust, and you enable the respectful, sharing culture that is so important to the way you market our province….

Failure to protect privacy, I should also add, can also lead to tremendous reputational harm, as Yahoo discovered following their massive privacy breach of more than one billion user accounts. Who here still has a Yahoo account?

Just as I thought. It will be very interesting to see how their market valuation will be impacted by this breach.

The tourism industry isn’t safe from privacy breaches, either. I’ll give you a few examples… last summer a cyberattack at a subsidiary of the Japan Tourism Agency gave hackers access to passport details and other records of nearly eight million customers… no doubt this was especially embarrassing given that Japan will host the Olympics in 2020.

Closer to home, a 2014 US survey of 1,000 frequent travellers showed that only 33% believe that their loyalty rewards information (credit card numbers, account data, and travel itineraries) were secure with airlines and hotels – hardly surprising following the apparent ease with which hackers stole credit card information for merchandise

returns from Target and Home Sense shoppers. Incidentally, that breach cost parent company TJ Maxx millions of dollars in direct costs, not to mention the cost to re-establish the credibility of their brands.

A hack last August at 20 Hyatt, Sheraton, Marriot, Westin, and other hotels in the U.S. proved that their fears were well founded. Data from the credit cards of an undisclosed number of people may have been collected for more than a year when they purchased food or beverages at the properties. Not great for establishing trust and building positive memories.

I wanted to also touch on “big data,” a tool your organization may be interested in leveraging as you research and market travel experiences.

My office is part of a number of ongoing discussions and research projects around the ethical and legal implications of big data. Just know this: however you’re using data, big or small, privacy legislation applies.

These rules shouldn’t be seen as a constraint on what you do, but rather as clear methodology for handling personal information, and for demonstrating to travelers and the public alike that the BC government and Destination BC, as a Crown corporation, respect their privacy.

Thanks for listening to me today. Technology will continue to grow, presenting challenges and opportunities to your organization. As you adapt with the times, we’ll be here to answer any of your questions.

I’d be happy to take any of your questions now, if we have time.