Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

SPEECH TO

SOCIAL MEDIA CAMP, VICTORIA

MAY 3, 2018

MICHAEL MCEVOY
INFORMATION AND PRIVACY COMMISSIONER FOR BC

Thank you very much for that introduction. I want to thank Chris Burdge for this very kind invitation to speak. I should say at the outset that Chris and I do have something in common – we're both members of perhaps the most legendary old men's hockey team known as the Victoria Grey Leafs.

That's where the comparison ends because your social media boot camp leader has far superior on-ice skills to the person standing before you.

I would like to extend my congratulations to Chris and his team who have put on this event since 2010.

Speaking of old-timers, I was around when BC's privacy legislation was developed way back in 1993. As I was thinking about what I would say today it occurred to me that if someone told me back in '94 I would be speaking at a social media camp I would have guessed that it was a friendly get together with my good friends in the press gallery – in those days we had a robust media and they were pretty social.

So much has changed since then.

Remember when people doubted how anyone could make any money on this World Wide Web "thing"? Today Facebook and Google are among the world's top five capitalized companies, each worth hundreds of billions of dollars.

Large or small, though, there are many, many tools now at your disposal to connect your organization, business, or public body or with citizens, potential customers, members, or users of your systems or products.

Looking at your extensive agenda over the past couple of days I see that you've learned about the best and worst of some of these tools—from fake bots and online story-telling… to how machines can teach us to be more creative… and finding solutions to your digital clutter problem.

What I would like to do with my brief time here is to change focus just a little. The message I would like to convey to you today is simple: how you use these powerful social media tools is incredibly important.

I can think of no more profound a philosopher to paraphrase than the great Spiderman, and say that with the great powers these tools bring to you comes great responsibility.

Why responsibility? When you use social media platforms to enhance your business, you almost always will be collecting people's personal information – and often that information can be very sensitive.

And when personal information is in play, my office will be there….

Let me now give you a quick primer on what our office is all about.

Many people ask me, "as commissioner – are you the government?" The short answer is, "no!"

I am an officer of the legislature. I share this designation with other officers, including the ombudsperson and auditor general. I am appointed not by government but by the whole of the legislature – government, the opposition, and the green party. And it has to be a unanimous appointment. That last point is really important because my job, among other things, is to hold government accountable when it comes to access to information and privacy. I also oversee private businesses and organizations like yours when you collect and use personal information. You can take my word, or the word of the other 39 people i work with, this is no small feat!

Under the *Freedom of Information and Protection of Privacy Act,* we have oversight of 2,900 public bodies in British Columbia... everything from government ministries, school boards, and police forces to health authorities and the like.

We are also responsible for the *Personal Information Protection Act,* or PIPA, which means we regulate more than 400,000 private sector organizations.

My office investigates and audits public bodies and private organizations. We also investigate and resolve privacy complaints. And when necessary, we issue binding orders.

We have plenty of sticks to enforce the legislation when we need them. But to truly reach out and get our message to the hundreds of thousands of organizations we regulate we also have to use the many carrots we possess.

Perhaps the main carrot – the one I think is most important – is educating and providing guidance about your obligations to protect personal information under PIPA.

You know, this couldn't be a more important time to talk about social media and the need to protect people's personal information.

A few weeks ago, I was in the UK helping the Information Commissioner there investigate a story you may have heard about in the news – a story involving a company called Facebook and another one called Cambridge Analytica.

Spoiler alert here – this investigation is still ongoing. I am sure you will not be surprised to hear I can't talk to you about any of the details.

What I can say, however, is that this whole controversy has raised awareness in the minds of the public and YOUR customers… an awareness about how companies use data – or sometimes, how they misuse data.

This new awareness is making people think twice about how they engage with companies like Facebook and other social media platforms. It's also turned a focus on all of you who use these platforms to engage and communicate with your customers and users and members of the public.

At the heart of all this is trust. For the benefits of these technological innovations to be fully realized, people must have trust – trust in social media platforms large and small and trust in those of you who use them. Trust that the personal information gathered about them is being used properly and in accordance with privacy laws, whether it's an email, phone number, birthdate, credit card number, location data, a like clicked for Justin Bieber, or an internet search for a sensitive medical condition.

The law you need to be most familiar with to protect your clients' or customers' data is the one I just mentioned a moment ago – PIPA, the *Personal Information Protection Act*.

I am not going to frighten you with a detailed dissection of this law. But you should at least be aware of its essence.

It's not complicated.

PIPA recognizes your need to collect and use people's information within reasonable boundaries, BUT (and that's BUT in capital letters), that information needs to be properly used and protected.

So within that simple statement are a few basic concepts.

First and foremost, to collect someone's information you need a legal basis. Those legal bases are set out in PIPA. The most important one for your purposes is consent.

In fact, it is often said PIPA is a consent-based statute.

So, how do you get consent? There are some obvious ways, as you might expect. One is to get express consent in writing. You could also get consent verbally, but this could be problematic if an issue arises at a later date about whether consent was actually given, and you might have competing recollections of a conversation.

Preferably, consent should be in writing, and it should state what a person is consenting to. It should also be clear, specific, and unambiguous. In other words, it should explain exactly how someone's information is going to be used – and for what purpose.

If I really liked the service your computer shop provided me and I wrote you a note to that effect I wouldn't necessarily think you would share that with the world on your Facebook page. If you want to use my testimonial, get my explicit consent, so that there is no doubt. Let me as the customer make the decision about what I want to share and for what purpose.

I'll add, however, that consent does not always have to be explicitly given. Sometimes it can be implied. If I give my hard drive to your computer repair business along with my phone number it would be reasonable for me to expect you would use the number to call me and let me know when the repair is done.

But what if you wanted to use that number to text me your latest iMac promotion? That would not be reasonably implied and certainly not what I would expect you to use the number for, again, unless you'd asked me directly.

Consent is a key ingredient when it comes to social media. When you post user-generated content like digital photography on your webpage or Facebook page make sure the customer is actually consenting to its use – and that they understand it might for example be used in the context of endorsing something you are selling or promoting.

This is precisely how Facebook got itself into trouble a few years here in BC. A woman named Ms. Douez clicked the like button beside what Facebook described as sponsored content – basically ads designed to look a bit like regular content in the newsfeed.

It's not clear if she even knew it was an advertisement.

Next thing you know Ms. Douez says her name and portrait were being shared among all of her friends essentially as an endorser of the product – but she gave no explicit consent to the company to do so.

Facebook has since changed the way it does this type of business, but this is a cautionary tale – be sure to seek clear consent.

One area of consent that I have to say is murky is consent based on very lengthy, overly legal, so called “terms of use” agreements. How many of you have had the experience of wanting an app and being asked whether you agree to the terms of use set out in fine print in a five-page document?

All you’re thinking is … give me the app!

Most of us just click “I agree.” But buried somewhere near the end of the five pages may be a line that says they can use your phone number to promote any company or associate company products to you – along with a proviso that they can sell your number to any third parties. Have you genuinely consented to these terms?

There are not a lot of cases on this point. I expect that under the new rules coming into effect in Europe this month under the General Data Protection Regulation this kind of agreement would not be considered valid consent.

I have focussed on consent as a very important way to collect personal information. But it is not always a magic bullet. You can’t use it for example to get information from a customer for things not required to provide the service.

Let’s say for example that you have an app that you have cleverly designed to sell flowers from your flower shop. I download your app and it asks me to give you my credit card to pay for the flowers – entirely reasonable – but now it is asking for my entire contacts list, without which I can’t get my flowers! Come on!

I am sure that would be fantastic for those of you out there to market more flowers to my friends, but in no way can it be said that you need those contacts for you to provide me with my flowers! It would actually also be contrary to the law!

So for the moment let’s assume you have properly collected my personal information – what are your obligations to protect it?

The first thing you should know is that you do have such a responsibility!

The law says you have to take reasonable means to protect my information. The risks in not doing so are very significant, and I stress again, it’s the law.

A data breach can seriously harm your customer or client. If their personal information is hacked, they could be exposed to identity theft or unauthorized credit card use, for example.

Data breaches can also harm your bottom line AND they can permanently damage the reputation of your business.

Just ask Facebook about that last one.

Facebook’s recent breach affected nearly 87 million users worldwide – 622,161 users in Canada alone – and wiped billions off the company’s stock value. I note parenthetically that my office along with the Office of the Privacy Commissioner for

Canada is currently conducting a joint investigation of Facebook and the BC-based company AggregateIQ.

At gatherings like this one, I'm often asked, "What can individuals do to protect information from being hacked or stolen from my social media accounts?" While it's always important to pay attention to your passwords, privacy settings and things like two-factor authentication – I'd like to pose a slightly different question as a regulator: "What are the social media and tech companies you're using doing on their end to protect our personal information?"

On that count I would have to say -- not enough.

The recent Facebook breach I just mentioned happened in 2014 and was in fact featured in an article in the *Guardian* in late 2015. Yet here we are, three years later, and Facebook is only now taking steps to notify its users that their personal information was taken without their consent.

The dangers of a breach apply as much to you and your businesses as they do to the big guys. Computer databases now allow even small businesses to retain a considerable amount of data, whether it is credit card information collected by a bed and breakfast or sensitive medical information at a cannabis dispensary. You must rigorously guard this information. As I noted a moment ago, the damage to your business would not only be monetary. Your business would also suffer long term reputational damage. People would just lose their ability to TRUST you.
When you ask your customers or clients for their personal information, you are essentially asking them for their trust. And trust is a currency that is very hard to get back if you lose it. Just look at Cambridge Analytica. Yesterday, the UK-based firm announced that it will be closing its doors.

So…. Privacy is good business.

But how do you privacy proof your business?

Well, thank you for asking. We at the OIPC are here to help! We have plenty of straight-forward tools to help you find your way. First, we recommend that you create a simple privacy management plan.

It doesn't have to be complicated, and to a large degree it involves common sense.

1. Take an inventory of the personal information you hold.
2. Ask yourself; is it necessary to collect and use this information in the first place. If not, don't expose yourself to unnecessary risk and safely dispose of it.
3. If you need to keep the information, ask yourself if you are properly securing it?

These are just a few of the questions you need to ask yourself.

I need to emphasize that privacy management plans are living, breathing documents. They require regular reviews and tweaks as your business evolves. We have guidance on our website at oipc.bc.ca to help.

Once you have a plan, you will want to distil it into a readable policy that you can share with people who visit your website. Don't be shy to tell your customers about it: In doing so, you are telling them that you are committed to protecting their personal information.

A good social media privacy policy should include what information you collect and use, such as customers comments, likes, content, and browser histories.

You should also include contact information for the person in your business who is responsible for privacy. Your customers may want to request a copy of their own personal information, which they are entitled to do under PIPA.

If you are scratching your head right now and thinking "We don't have a privacy person," now is the time to figure that out.

I can't emphasize enough that we are here to help.

As you pack up and leave the conference today, no doubt your head will be filled with ideas for engaging your customers through social media. I hope I've impressed upon you the need to build privacy protection into your business. The law requires it, but more than anything, it's good business, because it builds trust with customers, clients, and the public.

Thanks very much for your attention this afternoon. I'll close by inviting you to follow my office on Twitter @BCInfoPrivacy – yes, even the privacy commissioner is on social media.

I'm happy to take your questions now, if we have time.