CHECK AGAINST DELIVERY

Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

Luncheon Address to the Executive Directors and Registrars of Professional Organizations of BC – January 17, 2012

Technology and Privacy: *The Road Ahead*

Introduction

I would like to take the opportunity today to speak to you about technology, privacy, and the road ahead. I would also like to share my views on some of the issues that are currently keeping me up at night.

As we enter 2012, technology continues to raise opportunities and challenges for organizations like yours. As key decision-makers, you will have to make choices about which technologies to use and how you would like to use them.

To help public bodies and organizations make informed decisions, my office is developing guidance on technology-related issues such as social media background checks and cloud computing.

In addition to issuing guidance, I am carefully watching legislative developments that would increase the capability for law enforcement to conduct surveillance.

On a brighter note, I have watched as more and more public bodies use technology to bring information to citizens through open information / open-data.

Social Media Background Checks

As I mentioned, the decision about whether to conduct social media background checks is one issue that many employers are struggling with.

Way back in the last century (the 1990s), it used to be that an employer would gather some resumes and have a look at them.

Next, they would narrow down the applicants and conduct interviews. Towards the end of the process, they would check references. And perhaps – as an extra check, they might quietly ask around at social and professional functions to see if anyone had insider knowledge about the prospective hire.

As we all know, things have drastically changed.

Today, many employers begin Googling prospective job candidates as soon as their resumes hit their inboxes. Within seconds, an employer can usually pull up a hopeful candidate's photograph, and the search takes off from there.

The process of checking someone out online has a certain insatiable inertia to it. Image searches lead to blog searches. Blog searches lead to twitter feeds. Twitter feeds lead to Facebook postings, and so on.

With Facebook's new Timeline feature, launched about a month ago, curious minds can click on a particular month or year to quickly retrieve a snapshot of a precise period in a person's life. With this feature, employers can audit resume information and conduct targeted searches, such as digging for party photos by clicking on a candidate's birth month.

On January 10, Google introduced its "Search Plus your World" feature, which integrates Google+ social network content, including photographs, into Google search results.

In many cases, hopeful job candidates have no idea that this is going on. Social media background checks can seem like a casual thing. Staff can check candidates out on an office computer, a mobile phone, or a manager might decide to Google someone on his laptop in between periods of a hockey game.

But these checks are not casual.

The result can be that someone might not be hired because of something somebody saw online.

Or think they saw. A troubling variation is that an employer may discount a candidate because they have a skimpy online presence.

In other cases, a candidate may be rejected because some seemingly insignificant detail, such as their marital status, was enough to cause an employer to decide not to hire them.

In the US, a company called Social Intelligence Corporation will scour the internet for information about a prospective hire and deliver the results to an employer.

Last year, journalist Matt Honan decided to hire Social Intelligence to run a background check on himself.

His reporting caught the attention of Senators Richard Blumenthal and Al Franken, who have written an open letter to Social Intelligence asking questions about the company's practices.

In order to try to address the issue of social media background checks, my office has posted a guideline on our website. The guideline takes employers through the kinds of evaluations they should make before they click.

It identifies risks associated with social media background checks, such as collecting inaccurate information, irrelevant or excessive amounts of personal data. It also provides information about BC's privacy laws.

It may seem counter-intuitive, but just because someone posts information about themselves online it does not mean that an employer can legally collect it. It is also true that an employer has collected personal information if they view something on a screen but do not save copies.

Cloud Computing

Like social media, cloud computing is another area where I see organizations struggling, and with good reason.

By now, most of us know what cloud computing is – a form of outsourcing – but many entities are trying to figure out whether cloud computing is right for their organization, and if so, what that outsourcing relationship should look like.

Studies show that Canadians log more hours each week online than anyone else. We use cloud computing all the time in our personal lives in the form of services such as Gmail, Facebook, Drop Box and others.

With all of these services, we access software and data that is stored far away from the device that we are using to access it. In many cases, providers such as Google will store multiple copies of the emails we send to ensure that we can still access them in the event of a system failure.

These services have traditionally been used by private individuals in their personal lives. For the most part, the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* do not apply these kinds of communications.

Today however, public bodies and organizations are seeking out ways that they can use these same services, often because of their convenience and low cost.

The challenge is that privacy laws will apply, so entities must assess the risks carefully to make sure that any cloud computing relationship complies with the law and has adequate security.

These considerations apply whether the service is free or paid, whether the employee is using it from work or from home, and whether the data is being stored across the street or across the world.

In order to determine whether a cloud product will comply with privacy laws, organizations should use tools such as a privacy impact assessment to determine what personal information they want to offsite and where the cloud provider will store it.

Proper governance tools such as corporate policies and standards, along with rigorous contractual provisions, are key elements any time a public body or organization allows someone else to store their stuff.

Specifically, contracts should include a provision requiring a service provider to notify an organization immediately in the event of an actual or suspected breach. They should also include the right to conduct site visits and interview staff.

Professional regulatory bodies and other public bodies face a particularly significant challenge, as almost all of the major cloud providers are located outside of Canada. BC's FIPPA contains a unique provision that prohibits public bodies from storing personal information outside of Canada.

One of the few exceptions is if the public body has an individual's consent to store it outside of Canada, but this exception is more restrictive than many public bodies first realize.

For example, if a municipality wanted to outsource their employee's email to a US company, it would not be enough to get each staff member to provide consent to store their emails outside of Canada. This is because the rule requires the consent of the individual the personal information is about, and inevitably, emails will contain multiple individuals' personal information.

I am aware that public bodies find this challenging. My office will soon issue guidelines for the public sector on cloud computing, and we are working on resources for the private sector as well.

One resource that we already have available is an online self-assessment tool for organizations. Although we designed the tool for the private sector, public bodies can benefit as well. The online tool takes organizations through a series of questions, then evaluates how they are doing.

Lawful Access

In addition to the privacy risks associated with social media and cloud computing, lawful access legislation being proposed by the federal government has the potential to weaken privacy in Canada.

The term “lawful access” is a catchall phrase to describe a group of three bills. The first is Bill C-50, known as “An Act to amend the Criminal Code (interception of private communications and related warrants and orders)”.

The second is Bill C-51, known as the “*Investigative Powers for the 21st Century Act*”, and the third is Bill C-52, known as the “*Investigating and Preventing Criminal Electronic Communications Act*”.

The federal government introduced these bills but they died on the order paper last March. Many people are anticipating that government will re-introduce them when Parliament resumes in a few weeks.

Collectively, these amendments would change the way that law enforcement agencies can access our personal information.

My biggest concern is that they would allow police to collect data such as unlisted phone numbers, IP addresses, subscriber names and account details without a warrant.

In the view of Commissioners across Canada, the government has not provided evidence to support a conclusion that these intrusions on our privacy are necessary. In addition, the threshold for production orders has been lowered and in the case of subscriber information the evidentiary standard was eliminated.

Canada is not the only jurisdiction that is trying to make it easier for law enforcement to find out what we are doing online. In the United States, the House of Representatives is currently debating a bill known as the *Stop Online Piracy Act*, or SOPA.

The purpose of SOPA is to crack down on illegal downloading and the recording and motion picture industries strongly support it. The privacy problem with SOPA is that it would allow the Attorney General to compel internet service providers to block specific domain names, IP addresses or potentially, specific web pages.

In order to do this, those internet services providers may first need to examine where someone is going on the internet in order to block them from getting there.

This process of figuring out which sites and web pages someone is trying to get to is known as deep packet inspection.

SOPA would compromise Americans' privacy, because it would mean that internet service providers could be required to conduct surveillance on their customers.

This would capture information that may stop illegal downloads, but it could capture a lot of other information too.

In Spain, the government recently passed a law very similar to SOPA after receiving pressure from the US government.

Like SOPA, the Spanish law requires internet service providers to block access to certain web pages, which means that providers there must examine what individual subscribers are up to online.

Open Government

While lawful access is something that is keeping me up at night, the increasingly popular movement towards open information / open-data is something that isn't.

The basic concept behind open information is to make information publicly available so that individuals do not have to request it in the first place. For example, many departments in the US, such as the FBI and the CIA, have established electronic reading rooms.

In Britain, the government has a site that contains copies of government contracts and details of government spending.

Closer to home, the provincial government launched its own electronic reading room called DataBC last year.

The site contains information that various government ministries have chosen to make publicly available. It also contains copies of non-personal records that have been requested and released through the FOI process.

I am very encouraged and support open data schemes such as DataBC, and I encourage all of you to evaluate what they can do to promote open government.

The result is really a win-win situation: members of the public benefit from greater access to information, and public bodies save time and money by not processing the same FOI reques*t*s over and over again.

Recent Changes to FIPPA

Lastly today, I wanted to leave you with some practical information about recent changes to FIPPA that many of you may already be aware of!!!!

On November 14, 2011, the most significant changes to the Act came into force since the law was first passed in 1994. While there were many amendments, today I am going to focus on three of most significant ones.

First, the amendments to FIPPA include new requirements related to data-linking. Under the new requirement, public bodies that participate in data-linking must comply with regulations.

The definition of data-linking in the Act is new and it is broad. The essence of the change is that if a public body is going to combine one set of personal information in one database with another set of personal information in another for a new purpose, regulations will apply.

As of yet, no regulations have been prescribed, but it is something that government is working on and I anticipate that they will be coming soon.

A second significant change is that it is now mandatory for a public body to complete a privacy impact assessment and to submit it to my office for review, if it addresses a common or integrated program or activity or if it is a data-linking initiative.

In the past, only ministries were required to complete privacy impact assessments, and there was no requirement to submit them to my office.

We are currently developing guidelines on how to complete and submit a privacy impact assessment, and we hope to have that information up on our website soon.

Third, I wanted to draw your attention to changes in the Act that specifically authorize public bodies to use social media sites like Facebook to engage individuals in public discussion and to promote programs and activities. This opens the trans-border data door by a crack!!! The change should give public bodies confidence that they can use social media to engage citizens on an on-line dialogue.

Conclusion

In conclusion, I hope that I have provided you with useful information about some recent developments in privacy and technology. As a regulator speaking to a room full of regulators, I think we can all agree that keeping pace with the people and information we watch over is essential. I am looking forward to the road ahead.

Thank you for your attention this afternoon.