CHECK AGAINST DELIVERY

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Privacy Matters: Tips and Best Practices for IT Professionals

Elizabeth Denham
Information and Privacy Commissioner for B.C.

Keynote Presentation to the

Municipal Information Systems Association (MISA)
September 20, 2012

Good morning, everyone. It's great to be here.

Thank you Nelson for the kind introduction, and to the MISA BC executive for the invitation to speak.

I am inspired by this event – the setting, the size of the audience, and particularly, by the theme of the conference – devoting three days to discuss privacy and security!

I'm here today to talk about privacy, security and how you can implement privacy-positive data practices in your role as the IT gurus of local government.

But first, a bit of background for those of you who aren't familiar with my office and its mandate.

I am first and foremost a regulator.

The Information and Privacy Commissioner is an independent, non-partisan officer of the Legislature.

My job is to enforce the *Freedom of Information and Protection of Privacy Act.* The law governs the information practices of more than 2,900 public bodies, including local governments.

I also oversee the privacy practices of the private sector. The *Personal Information Protection Ac*t applies to more than 300,000 businesses and non-profits in the province.

My office is made up of a team of investigators, lawyers, policy analysts and a technical analyst!

I have investigative and audit powers, and the mandate to make public comments on programs, policies and services affecting information and privacy rights in BC. I can make orders that are legal and binding.

I also have a public education mandate. Not every regulator has a public education mandate, but I do.

I strongly believe that making citizens, public bodies and private organizations aware of their rights and responsibilities, is an essential part of my work.

As you can imagine, I spend a lot of time in rooms like these talking about the value of privacy.

And for good reason.

Privacy is really important!

And I'm not just saying that because I'm the Privacy Commissioner.

Without privacy, we wouldn't have freedom of association, or freedom of expression.

Without privacy, we would not have the ability to decide what we choose to share of ourselves with others.

In respecting the privacy of one person, you are securing your right, and the right of others, to do the same.

Of course, there are some who disagree.

Facebook founder Mark Zuckerberg once stated that privacy as a social norm was no longer relevant.

The culture has changed; we are no longer concerned with privacy and "the right to be left alone."

Unfortunately for Mr. Zuckerberg, the actions of citizens have proven that sharing technologies like Facebook, social media and the Net have brought about a bit of a privacy renaissance.

AND… citizens are using these technologies to take action in defense of their privacy rights like never before.

Those of you who are on Facebook are probably used to seeing posts like these in your News Feed.

This post is warning users about how Facebook is allegedly using photos for third party ads and how to change your privacy settings to prevent this activity.

Of course, not every one of these posts is 100% accurate.

And some of these posts are just downright hilarious.

But there is no question that the viral nature of these type of privacy-related public service announcements, posted and re-posted across the social platform – gives you a sense of how these technologies are being used to raise awareness about privacy risks and intrusions.

Another example is the campaign to stop the federal government's Bill C-30 – aka "lawful access" – that if passed would permit, among other things, warrantless access to subscriber data held by internet service providers.

To date, 145,000 people signed an online petition organized by a Vancouver advocacy group.

Then there was the Twitter campaign that followed Bill C-30's introduction in the House of Commons. Canadians expressed their dissatisfaction by posting the inane details of their lives under the hashtag #TellVicEverything "Vic" being Vic Toews, the Minister of Public Safety).

On February 16, two days after the Bill was introduced, #TellVicEverything was the top-trending topic in Canada, and #11 on Twitter worldwide.

Or consider the anti-SOPA protests that happened across the border in the United States.

115,000 websites including Reddit and Wikipedia joined in a one-day online protest against the anti-piracy law on January 18, 2012.

On that date, 3 million people emailed their representative in Congress, 2.4 million people Tweeted about SOPA, and a petition at Google logged 4.5 million signatures in opposition to the Bill, which has significant implications for the rights of citizens in the United States and worldwide.

These movements prove that despite advances in technology, citizens care deeply about their privacy.

In fact, technology has made these issues much more personal – not just because technology opens up new avenues for collecting, using, and disclosing personal information. But because these technologies are in the hands of individual citizens – meaning that the relevance of questions like: who has my information and what are they doing with it? All of a sudden become much more real.

There is no question, that these new technologies have made protecting privacy more difficult – because they open us up to certain risks. Privacy breaches. Identity theft. And improper or unauthorized access to data – both accidental and deliberate.

A growing number of public and private organizations look to IT to play a leading role in protecting privacy and securing personal information.

Some of you in this room may already be wearing this hat.

In a way it makes sense. Technology is the new frontier in privacy protection and enforcement. And of course privacy is simply not possible without security. Privacy presupposes a secure environment.

We often hear that the challenge facing today's information and security professionals is, "getting the right data to the right people at the right time."

I would add that it has to be done IN THE RIGHT WAY.

It has to be done in a privacy protective way, one that provides for robust security as well as authorized access.

At the end of the day, citizens will be relying on you to ensure that the tools, systems and technologies are in place to protect their information.

After all, given the complexities of data governance, the explosive power of analytics and the lightning-quick evolution of technology how would the public even know what to complain about?

With that in mind, I want to impart to you some of the concepts, principles and practices you can use to promote privacy and security in your organization on behalf of citizens.

I'm going to focus on two concepts for today: reasonable security requirements and accountability.

As some of you probably know, the *Freedom of Information and Protection of Privacy Act* sets out the conditions under which public bodies can collect, use and disclose information.

But it also creates a legal requirement for public bodies to protect and secure personal information in their custody.

A public body must have the appropriate administrative, physical and technical safeguards in place to protect personal information against risks like unauthorized access, theft, accidental disclosure or improper disposal.

But "reasonable security" is not a one-size-fits-all standard. Because situations vary, the measures needed to protect personal information will vary.

The measure of adequacy varies depending on:

- the sensitivity of the personal information;
- the medium and format of the records;
- the costs of security; and
- how valuable the information might appear to those intending to misuse it.

As a regulator, we assess a public body's compliance with "reasonable security":

- in response to a privacy breach;
- in the course of investigating a complaint; and
- in a Commissioner-initiated investigation or audit.

Usually, you know you are going to have a bad day when my investigators show up. In every breach investigation, IT is involved.

That's reasonable security in theory. I want to walk you through some of our more recent investigation reports to show you what it looks like in practice.

These cases are also helpful in terms of helping you to understand what my office expects of you, in the wake of an investigation or audit.

In January 2012, thieves broke into the Administrative Services Building at the University of Victoria. One of the items stolen was a USB flash drive containing the names, SIN numbers and banking information of 12,000 current and former employees.

This was a significant privacy breach affecting thousands of British Columbians. Current and former employees were deeply worried about their exposure to bank fraud, identity theft and other harms.

UVic reported the breach to my Office, and I decided to launch a comprehensive investigation given the severity of the breach and the number of individuals affected.

We examined the University's compliance with "reasonable security" arrangements – the requirement in law.

What we found was that the University was aware of its obligation to safeguard sensitive personal information using a range of protective measures.

They had sound fundamentals of data governance: they appointed a privacy officer, approved a privacy policy, and had completed training workshops to raise awareness about privacy and security at the University. All very important stuff.

BUT there was no clear policy, or direction to establish a sufficiently high standard for protecting the type of information stored on mobile devices like laptops and USB keys. A critical area of vulnerability in all organizations.

Portable data storage devices are extremely problematic!

Given the method of storage – a portable device – and the sensitive and confidential nature of the information – we determined that encryption – not just password protection – is the minimum security standard.

Because UVic had failed to implement this level of protection, they failed to meet the "reasonable security" test under section 30 of FIPPA.

So, what is the take-away here?

We can't prevent malicious activity BUT encrypting data on the mobile device would have ensured a much more benign outcome! A relatively simple but preventable error resulted in a privacy breach with ENORMOUS costs in time and money for the university and its employees.

I encourage each and every one of you, if you do not already have a policy or directive governing the use and protection of data on mobile devices – including laptops, smart phones and USB keys – to implement one as soon as possible.

Make sure your employees know about, and are trained to follow the policy.

And if you have already implemented a policy, I would encourage you to take a close look at how and whether your policies are being followed. Ongoing monitoring is essential.

This next example was quite a memorable one for me – given that it happened during my first week as Information and Privacy Commissioner for BC.

On July 16, 2010, BC Lotteries launched a new online gaming platform called PlayNow.com.

On the date of launch, because of a software glitch, sensitive customer details, including names, bank account and credit card numbers, were displayed to other PlayNow customers.

My office initiated a two-part investigation. First, we assessed the privacy breach that occurred on the 16th of July. Second, we launched a second, more detailed investigation that examined the general security of the PlayNow platform. BCLC referred to this as a "data cross over".

This was the first time my office had ever investigated an online platform, and addressed the unique security considerations a public body must take into account when moving services on-line.

Online platforms have privacy and security risks that are not common to other systems such as phishing, malware and spyware.

Government's involvement with gaming requires an increased level of trust and confidence on the part of customers. With this increased level of trust comes an increased level of responsibility.

Finally, given the circumstances, I found that online systems require proactive and ongoing monitoring, testing and training to ensure policies, procedures and systems are up to date.

After examining the security of the online platform, we found that BC Lotteries failed to have reasonable security arrangements in place when PlayNow was first launched.

The individual deficiencies uncovered by our investigation – including user access and malicious code controls, inadequate processes for system patches, and some unencrypted data transmissions – may not on their own trigger a failure in the "Reasonable standard" test.

But taken cumulatively, we found that there was not a reasonable level of security in place when PlayNow went live.

The site was down for nearly five weeks while BC Lotteries addressed the deficiencies – at their estimated cost of $150,000 dollars a day in lost revenues.

One final example that most of you will likely be familiar with.

BC Hydro is in the process of installing smart meters for its more than 1.8 million customers. Many of you likely have a smart meter installed on the side of your home.

Once fully operational, smart meters will provide hourly information about household electricity consumption, and transmit that information wirelessly to BC Hydro.

In 2011, as a result of hundreds of submissions made to my office by concerned citizens, I initiated a comprehensive investigation of the privacy and security aspects of BC Hydro Smart Meters.

People were concerned that BC Hydro was collecting data about what they were doing in their homes and what third parties might be doing with this data.

Among other things, our investigative team examined whether the smart meter initiative met FIPPA's standards for "reasonable security."

Given that smart meters are a new technology that collects personal information from its customers more frequently – in this case energy usage on an hourly basis – we interpreted "reasonable security" to require a high level of rigor.

Because smart meters and the smart grid aren't yet fully operational, we conducted our evaluation of "reasonable security" based on existing safeguards as well as plans to secure the data in future phases of the project.

After examining the administrative, physical and technical safeguards that are in place, as well as those planned by BC Hydro, we determined that the security arrangements met the requirements under section 30.

This was a more difficult investigation to carry out. Because smart meters and the smart grid are not yet fully operational, we could only comment on concepts and planned architecture.

This file is <u>on active watch with my office, as BC Hydro implements future phases of the project</u>.

These case examples show that “reasonable security” is not a one-size-fits-all standard.

The key to compliance is a thorough assessment of your own operating environment.

Careful consideration of the different factors at play – including risk, technology, and the type and sensitivity of personal information collected – is critical. As is ongoing evaluation to ensure those processes are being followed.

Accountability

So, how can you as an IT professional promote compliance with privacy law?

The solution is not to say “no” to new technologies, or to turn a blind eye to these challenges. It is to embrace them in a privacy-protective way.

The solution is to create a privacy management program to address these issues…to lay the groundwork…BEFORE systems are built.

It’s the process, not the project.

A privacy management program is a constellation of policies, controls and best practices that work together to protect and secure personal information across the board.

You have to consider privacy before design.

Fortunately, just as IT has its own standards and certifications which we can base best practices, Privacy Commissioners across Canada have collaborated to develop some best practices – a framework if you will – to help you create a privacy management program for your organization.

It’s called “**Getting Accountability Right with a Privacy Management Program.**”

The paper is practical, workable and scalable and will help you demonstrate accountability and better protect personal information.

While the guidance is geared towards private sector organizations, it is equally applicable to local government.

We are currently drafting a companion set of guidelines, specifically aimed at BC Public Bodies.

But in the meantime I want to walk you through the paper's "building block approach" to privacy management.

By implementing these building blocks, you can demonstrate to citizens, to elected officials, and regulators that you are committed to privacy and accountability, enhancing your reputation and building trust in those relationships.

The building blocks begin with corporate organizational commitment to develop a privacy-respectful culture.

This has to start from the very top – with buy-in from senior management.

Only then, can responsibility be truly delegated to a Privacy Lead, perhaps supported by a team with delegation and clear roles and responsibilities.

Next are the program controls, starting with an inventory of what personal information you hold, where it is held, its level of sensitivity and the purposes for which it is being collected, used and disclosed.

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

The bottom line: Privacy management is not a one-time thing, or a one-off. You can't say, privacy, yeah, we took care of that in 2004. It takes a fundamental commitment, supported by a strong team that includes IT.

An investment in privacy and security up front is a far better bet than cleaning up the mess after a catastrophic data breach, which could be as simple as a lost USB key—a costly way to erode public trust. [1]

Some of you in the audience might be thinking, sure – easy for you to say from up there … but how can I actually apply privacy management? Where do I start?

First things first. Build a culture of accountability along with other key decision makers in your organization.

---

[1] Just a footnote of interest. Yesterday some recent stats out of Alberta – in the first two years of mandatory breach reporting to the Commissioner there were 63 reported breaches:

- 22 breaches were caused by human error (most common mail and courier issues);
- 18 breaches caused by theft (loss of computer devices in cars in particular);
- 14 breaches caused by electronic system compromises (typically found to occur as a result of targeted attacks by external hackers seeking data); and
- 9 breaches caused by failure to control access to electronic files (files erroneously posted to the Internet).

Designate a privacy officer. Support their work across the company to build a robust privacy 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.

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.

Is your data stored and accessed ONLY IN CANADA? The law prohibits transborder data flow (with some exceptions).

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.

Some further advice to minimize impact of a breach – basic steps:

1. **Limit collection of personal information** to only what is reasonably required.
2. **Develop policies and procedures** with privacy in mind, and update regularly.
3. **Train staff to understand** the importance of personal information and of breach notification.

These are just a few examples of how the accountability tool can be made to work for you.

The tool is available for download on our website; there is a two-page primer as well as the full document with guidance.

I also encourage you to check out our interactive security assessment tool, and our guidelines for cloud computing.

We also have extensive guidelines for breach management and reporting.

Thank you for your attention this morning. I hope that you have a better understanding of some of the concepts and principles at play when we're talking about privacy, security, technology and personal information management in BC.

I'm happy to take a few questions from the floor.