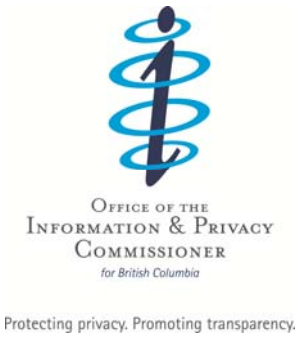
CHECK AGAINST DELIVERY



Information & Privacy Commissioner Elizabeth Denham's
April 4, 2011 keynote address
to the Privacy and Cloud-based Educational Technology Conference

Finding Our Way Through The Clouds

Thank you for that kind introduction.

Introduction

The pressure on BC's academic institutions to deliver world-class learning environments and services is huge. Staff are in a constant state of having to try and do more and more with less and less. Increasingly, institutions are exploring products that promise software as a service, platforms as a service and infrastructure as a service. According to a 2008 US study, 69% of online Americans have used at least one kind of web site that operates in this way.

Organizations that provide these services often tell customers that they can offer flexibility at a low price. The question on everyone's mind is whether to buy and if so, how much to buy.

At the same time, social media has just exploded. There are now about 200 major social networking sites worldwide and several boast tens of millions or, (in the case of Facebook), hundreds of millions of users. The topic of how these networks are transforming our educational institutions is particularly fresh and we are only beginning to understand some of the implications. Can instructors use Facebook to teach? Can they base participation marks on wall posts or blog entries?

Academic institutions should reflect the societies they serve, and it is clear that Canadian society is online. According to a global study released in March, Canadians spend an average of 44 hours per week on the internet, which is more than anyone else in the world and almost double the global average of 23 hours per week. In the US, the weekly average is just 35 hours a week. I think this is amazing.

Recent Canadian Examples of Outsourcing

In Canada, we have two recent examples of academic institutions adopting an outsourcing model.

In December, the University of Alberta announced that it had entered into a four-year contract with Google to provide students, faculty and staff with Google-based Gmail, calendars and document preparation tools. Under the agreement, students and staff will retain their @ualberta.ca email addresses and will not encounter any advertising from Google. In addition, the University says that Google has agreed not to conduct data mining of any of the emails. Under the agreement, mailbox size will increase from 1GB to 7.5GB. According to the university's website, the emails will be stored on Google servers located all over the globe.

In February, the University of Guelph contracted with a third party, Scalar, to provide web-based email and calendar services to students and staff using Zimbra. Whereas Google will store the University of Alberta's data on servers located around the world, Scalar claims that emails and other data from the University of Guelph will only ever be stored on servers located within Canada.

These institutions have taken the plunge, and clearly, from the turnout today, this is an issue that many academic institutions are grappling with. Other sectors are struggling with this issue as well. For example, last fall, the Law Society of BC formed a working group to consider offsite electronic storage of records to third parties.

Similarly, the issue of how and whether educators can compel students to use web-based third party applications like Facebook is different from the issue of how and whether institutions should outsource their email, but I think many of us conceptualize these problems in a similar way. These are new issues. Facebook and Gmail haven't even celebrated their 10th birthdays yet! Outsourcing infrastructure is fairly new as well. *Everyone*, not just academic institutions, are trying to figure out what to do.

How the Internet is Changing

Traditionally, institutions purchased software, paid annual licensing fees, and installed software on campus computers. If students had their own computer, they might be able to purchase the software at a discounted rate to use at home. If they went out of town for spring break and they didn't have the right software on their computer, the student was out of luck if they wanted to work on their term paper, not that any student would actually *want* to do such a thing during spring break!

This is all changing. Companies like Google offer software not as a product, but as a service. With Google Docs, the student can be on any internet-enabled device and can work on that darn term paper. It can be a PC or a Mac. It can be a phone or a tablet. It doesn't matter, because the content is on Google's servers and can be accessed from anywhere.

Better yet, if one student is on campus for spring break and another student is in Mexico, they don't have to email each other versions of their group project, they can work on it together at the same time from anywhere, because it is all in the same spot. The paper isn't on the student's computer, memory stick or disk – it's on Google's servers.

And this is wonderful but it is also challenging, and I think that is why we are all meeting together to talk about this today.

Last year, Columbia University law professor (and former IBM computer programmer) Eben Moglen delivered a speech about cloud computing at a meeting of the Internet Society's New York branch. Although his speech was called "Freedom in the Cloud", he didn't use the term until well into his talk. When he first uttered the word "cloud" he was quick to say that he thought it didn't really mean anything. Instead of talking about the "cloud", Professor Moglen talked about servers, logs, and ownership of data.

In terms of privacy considerations, I think that speaking about servers instead of clouds is the right way to go. BC is no different than dozens of other jurisdictions around the world: there are laws about what you can do with other people's information. You have to keep it safe. You can't let people see it, copy it, use it, disclose it, or dispose of it unless they are allowed to. You have to let people see the information that you have about them. You have to make sure it is accurate if you're going to use that data to make a decision that is going to impact them. These sound a lot like service standards, and often they are, but they are also laws. Everybody wants to provide reliable service, and everyone wants to comply with the law.

One issue that comes up frequently is the provision in BC's *Freedom of Information and Protection of Privacy Act* ("FIPPA") that limits the disclosure of personal information outside of Canada. The BC Government passed this provision as an amendment to FIPPA after the US government passed a series of amendments called "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" also known as the USA PATRIOT Act.

The reason the BC government did this was because under the USA PATRIOT Act, American authorities can obtain orders from a secret court called the Foreign Intelligence Surveillance Court to compel any company under US jurisdiction to hand over the information they are storing and they are prohibited from telling anyone about it.

Other jurisdictions in Canada, including Alberta, do not have these restrictions. My sense is that people think that because BC has these restrictions, they can never send personal information to the United States. That is not entirely true – for example, public bodies can store personal information outside of Canada if they have an individual's consent to do so. But really, I think that people should put this provision aside and make room to consider all of the other privacy considerations that fit into the equation. Things like security, retention, unauthorized disclosure, and access.

As the recent example from the University of Guelph shows us, there are corporations out there who are responding to Canada's public and private sectors when it comes to managing data. Last April, Ontario-based CentriLogic said it was introducing the first service that supported organizations that needed to ensure their data did not leave Canada. IBM launched a similar Canada-only service earlier this year as well. Both companies identified data residency concerns as a reason for offering the service.

Another Canadian-based company is doing something different all together. In February, Enomaly launched the world's first "spot market" for cloud computing. The system is very similar to sites like Hotwire.com. On Hotwire, users purchase hotel rooms for a certain amount of time in a certain city at a discounted rate. They don't know where they are staying until after they've purchased the room. The reason for this is so that leading hotels can still try to sell

rooms under their brand at higher rates on other sites. The customer pays more, but they also know where they are staying before they buy the room.

On Enomaly's Spot Cloud market, buyers and sellers log onto the market site using their Google account. They can select the kind of storage they want and the number of hours they want it for, then purchase it by debiting the transaction to a pre-paid account with Enomaly. The site offers no returns, and most significantly, buyers never find out who the seller is, even after they purchase the storage. Enomaly takes a percentage of each transaction.

On its website, Enomaly instructs buyers that they must use the service at their own risk. It's a bit like being driven from the airport to your hotel with a blindfold on. If the place is messy or dangerous, there is no front desk to complain to. The trade-off is that you can get that room for a steal.

Although this service allows buyers to determine where they want to store their data, it does not allow them to know where their data is, who has it, or what they might be doing with it when it is on their servers. This is an example where data would be stored in Canada, but it is not at all apparent that it would meet the security, accuracy and retention requirements set out in FIPPA.

Another issue that comes up with outsourcing is that stealing servers is a lot easier than stealing actual clouds. This is not a new concept, as people have always been able to steal computer hardware. It does add new complexity however, because with outsourcing, the data is once removed from the entity with primary responsibility for the information.

In the summer of 2008, IBM announced that it had signed a five-year, $300 million dollar deal to manage data and provide other IT services to US-based insurer Health Net. At the time of the announcement, Health Net COO James Woys said; "This is an important step in making Health Net more competitive and is a key component of our operations strategy to increase our capabilities while reducing administrative costs and improving efficiency."

Fast-forward to 2011. Exactly one month ago today, on March 4, Health Net called the Connecticut attorney general's office and told them that nine of IBM's server drives in Rancho Cordova California had been missing since early February. Health Net said that the server drives contained the personal information of almost 2 million current and former customers, employees and health care providers, 24,599 of whom live in Connecticut. The California-based company called the Connecticut attorney general's office because under the terms of a lawsuit settlement stemming from another massive breach involving 1.5 million customers in 2009, Health Net was required to notify officials in that state if they ever compromised their customers' privacy again.

Although Health Net has not yet confirmed publicly exactly what information is missing, it has said that the information could include names, addresses, health and financial information, and Social Security numbers. Health Net is in the process of notifying all affected individuals. California's Insurance Commissioner Dave Jones is investigating.

I want to shift a bit now and get back to the issue of Facebook in the classroom. I think one thing educators need to consider is the degree of control they have over something like that. If an educator wants to administer a Facebook page for students, how do they know that it is really the students they are letting join the site? It might be Mary's smiling face next to her name

on that request, but how can you be sure it is really Mary? Educators should also consider whether their activity violates Facebook's terms of use.

I read a wonderful story in Victoria's *Times Colonist* newspaper last month about a Victoria police staff sergeant named Darren Laur who posed as a teen on Facebook in order to educate students about privacy. Laur, who is 46, maintained a fake profile for over a year on Facebook using purchased pictures and information gleaned from the Facebook accounts of real teens. When he made a presentation at Cedar Community Secondary in Nanaimo last month, he had already friended 30 students at that school who had no idea that their "friend" was actually him. He had done such a convincing job with the profile that one of the real teens even asked the fake teen out on a date. When Laur revealed during the presentation that *he* was their friend, students were shocked and pledged to pay more attention to their privacy online.

There is also the question of whether using Facebook to educate students is effective. In one US study from 2010, researchers evaluated the effectiveness of using Facebook as part of a course for Pharmacy students. The students were asked to join a class group on Facebook and were given instructions to make a certain number of postings on a given topic. At the end of the course, researchers asked the students to provide feedback on their experiences. Some of the students reported feeling more comfortable posting online than speaking in class. Other students reported a greater understanding of how what they posted on their own Facebook profile could impact their professional reputations. At the same time, students complained that because of the Facebook group, they had to check both the course's home page and Facebook for updates and instructions, and they found this tedious. The researchers also noted that although 75% of the students checked their own Facebook account every day, none of them checked the class group that often, and most only checked it a few times per month.

Facebook is just one of the many possibilities available to instructors for collaborative online learning. I think that whether you are an IT manager examining whether to outsource, or whether you are an instructor considering using Facebook, you need to think about where the data is going, why it is going there, and who has control.

Conclusion

In February, US Secretary of State Hillary Clinton spoke to students at George Washington University about internet freedom. She told the group that countries, businesses, civil society groups and digital activists must continue to work together to promote internet freedom and to address issues such as how to handle privacy in the context of cloud computing. I think that we also need to take a collaborative approach to address these issues here in Canada. We need to work together to create solutions that allow us to benefit from technology while protecting our privacy.

Thank you for your attention this morning.