Privacy and Cloud-based Educational Technology Conference Final Report

April 13, 2011

Summary of recommendations

Approximately 100 participants from B.C.'S post-secondary institutions gathered at BCIT in downtown Vancouver Monday April 4 to learn about and discuss issues of Privacy and Cloud-based Educational Technology.

Conference participants asked BCcampus to forward a summary of the discussions at this meeting to the Office of the Information and Privacy Commissioner, to assist in identifying mutual issues to form the basis of an ongoing dialogue.

In general, the tone of the conference was one of accepting the responsibility of enhanced freedom at all levels: personal, professional and academic. Most conference participants advocated for closer ties between the "real" and "virtual" world - pointing out that as technology advances and societal norms change, standards of conduct should be the same in each. There was a general sense that the FIPPA legislation, and in many cases institutional policies surrounding digital privacy issues, have not caught up to this paradigm shift.

As we reported in the background paper "Privacy and Cloud-based Educational Technology," we detected at the conference that the current education environment around this issue is a mix of fear, confusion, indifference, anger and frustration. Many students and instructors find restrictions around use of social media in education absurd given that they are already using the applications for personal use.

We have tried to capture all the recommendations submitted from the small group discussions at the conference accurately (those are the numbered recommendations). Some small group reports, however, were little more than "jot-notes" that were incomplete or lacking the context of the discussion. For the sake of clarity and readability some of those types of submissions were omitted.

Cloud-based educational technologies provide cost savings and open up educational opportunities and practices that improve the quality of education and cannot be achieved any other way. B.C.'s public post secondary institutions want to take advantage of both the cost savings and the educational opportunities but are being constrained from doing so by FIPPA.

Institutions are seeking ways within the bounds of legislation to do both, but the gap between what the legislation says and what many are doing in practice is significant. This creates a need to either:

a) change the legislation;

b) educate practitioners on what is allowed and what isn't;

c) understand the value proposition associated with practices that don't comply with legislation;

d) define processes that work within the law;

e) all of the above.

The clearest recommendations heard at the conference encompassed "all of the above" and were as follows:

1) to work with the Office of the Information and Privacy Commissioner and, if possible, the Office of the Chief Information Officer to develop a set of policy guidelines and resources for post-secondary educational institutions (post-secondary sector, as facilitated by BCcampus);

2) to act as a resource, convener and facilitator on this issue for B.C.'s post-secondary system (BCcampus);

3) to review amendment 30.1 of the FIPPA regarding storage and access of personal info to provide provisions to include social media specifically (government).

Detailed Summary of Small Group Reports

Question 1: What are the top three actions the government could take to help clarify the privacy legislation for the BC public post-secondary system?

Legislative change:

Conference participants noted that B.C.'S FIPPA legislation is more stringent than other Canadian provinces and in the United States, and wondered why we are so different. Many were surprised to hear from keynote speaker Caitlin Leminsky from the Office of the Information and Privacy Commissioner that the five-year review of the FIPPA legislation had recently taken place.

The majority of conference participants were of the view that the post-secondary sector should advocate for changes to the legislation as a sector, namely:

1. Review amendment 30.1 regarding storage and access of personal info to provide provisions to include social media specifically.
2. Shorten the period between reviews of the legislation, or at least publicize more widely the review process.
3. The amendment based on the U.S. Patriot Act should be repealed to drop the requirement that data must be hosted in Canada unless with specific consent.

There was not unanimous agreement among conference goers that B.C.'S privacy legislation was too stringent. A small minority of participants called for a single, federal, pan-Canadian piece of legislation around FIPPA that is at least as strong as is found in the European Union.

Guidance and clarification:

Conference attendees looked for clarity on what they can and cannot do under the current privacy legislation, but heard from the OIPC representative that the OPIC cannot issue specific advice or "clearance" to use certain technologies. Because the OPIC is in charge if investigating complaints, it would be inappropriate for that office to approve specific uses; they may have to adjudicate that same practice later if a complaint is made. "It's frustrating because technology is changing so fast, we can only get opinions and recommendations, not straight rules and regulations," reported one discussion group.

However, the OPIC does have a mandate to educate the public about FIPPA, and the OPIC representative agreed to work with B.C.'s post-secondary sector to develop some guidelines where appropriate.

Conference participants reported that the FIPPA legislation "feels deliberately vague. We are all trying to comply with something but there are no lawsuits to reference so we know what to do." One small group noted a paradox: post-secondary institutions spend resources and make decisions under rigorous FIPPA legislation that is complaints-based, yet the evidence [as noted in the video presented by the Digital Tattoo Project] is many students say they don't really care about giving their private information to social media sites they use regularly.

"We shouldn't have to wait until a student files a complaint and we're found in breach of a policy before we learn what to do," reported a discussion group. Not surprisingly, the conference had many recommendations around guidance and clarification about FIPPA:

4. The number one recommendation from conference goers on this issue of guidance is for the OPIC to work with the post-secondary sector (as facilitated by BCcampus) to develop a set of policy guidelines and resources for educational institutions.
5. More resources (possibly a hotline) provided by government to be used by post-secondary institutions that have questions around FIPPA. What privacy resources are available for low resource institutions that do not have a privacy officer?
6. Examples of what to do in certain situations; use cases outlining specific examples of how institutions and students can comply with FIPPA.
7. Many small groups asked for clarification on the following questions and issues:
    - Concern liability is cumulative and not sure when you may have crossed the line: who makes the policies and enforces them? What are the repercussions for not following them?
    - Can informed consent happen when a student is already registered for a class? Can consent happen at time of admissions or registration and thereby provide a blanket agreement regarding downstream use in courses or other educational activities?
    - Need help identifying what privacy statements include, what applies to K-12, Post Secondary.
    - Larger than just FOIPOP - directive on how to handle data
    - Can you proceed on your own (as VCC did) just because nobody has complained?
    - Develop case studies to clarify - Ministry of Citizen Engagement
    - Why want Government CIO on this? If this is serious why isn't the government enforcing?
    - Provide PSIs with FAQs, guidelines, workshops, designed to increase level of awareness about how privacy laws intersect with use of social media., from the perspective of teachers, students, IT professionals.
    - Larger than FOIPOP - just generally how to handle data - have expert available to answer our questions - a straighter line to answer questions [about the legislation]
    - Is there a dialogue occurring between copyright and privacy specialists in government and if so, can this be shared with the universities/colleges? Is this dialogue occurring on B.C. campuses?

Funding:

A couple of the discussion groups pointed out the resource limitations of monitoring everyone in their institution for possible breaches of FIPPA, and of having alternatives to cloud technologies available that are hosted at the institution. Post-secondary institutions are not resourced to be responsive to rapid changes in technology. One conference discussion group asked for government to "provide budget designed to provide equivalent innovation services without cloud computing." However, most groups asking for more funding asked that:

8. Funding be provided so BC institutions could set up "cloud" services with servers in British Columbia.

Question 2: What are the top three actions the BC public post-secondary system can take to maximize the potential of cloud-based services while protecting students' privacy?

Conference participants expressed a need for B.C. institutions to take a collective approach to this issue, and their diverse recommendations spanned technical, policy, research and educational solutions. There was a very clear need for the system to collaborate and pool resources and knowledge around issues of privacy and educational technology. Following is a summary of the recommendations conference-goers had for the post-secondary institutional system.

System-wide technical recommendations:

8. BCcampus explore consortium model for B.C. based cloud solutions to offer to B.C. universities and colleges (look for Canadian based solutions and open source products)
9. Use Open ID, it provides a protected, encrypted authentication system for sites which require users to sign-on who are participating in this system.
10. More B.C./Canada-based services created locally
11. Institutions all encrypt content that goes into the cloud (reasonable protective measures)
12. Automate masking/"pseudonymization" or aliases - so it's easier to "anonymize" data BUT if we encrypt we control it too tightly, we're severely limiting the concept of the personal learning network.
13. Privacy protection schedule - something we can get added to our contract with Elluminate so it Patriot Act minions came after it, Elluminate would have to tell us.

Research:

15. In order to compliment the cost savings argument for the use of social media – develop the educational benefits of social media in the classroom.
16. In order to assist our understanding of the relation between privacy legislation and use of social media in the classroom, complete comparative research looking at different provincial privacy legislation and the different social media educational advances in the provinces.
17. Collect more data about students' concerns about privacy.
18. Look at jurisdictions with strong privacy laws (eg Europe) and how post secondary institutions operate in those jurisdictions.

Policy:

19. Develop institutional-level social media policy and consent approaches to complement the classroom-based VIU approach.
20. As institutions promote the use of social media in the classroom and as we spread the notion of where/when education occurs, clarify the institutional responsibility for student's use of social media "in the space in between the classroom" – that is in the space students experience beyond the classroom.
21. Acceptable use policy and informed consent should be introduced very early on in a student's lifecycle, at the admissions process or when the student first registers. This could be similar to the acceptable use IT policy students have (at UBC). This may have accessibility issues which need to be addressed.
22. When embarking on a project we should always take into consideration what the privacy regulations are.
23. Need to be accommodating so that we can give them [students] a choice whether to use cloud/social media or not.

Shared Resources/Professional development:

27. Ensure all privacy officers are communicating up to date information with each other.
28. Provide guidance about specific software, for example, what you need to know about Facebook's privacy statement. Instead of having each instructor read and understand this (which was recommended earlier), you should have one person (or the privacy officer) per institution (or B.C.-wide) read and understand issues for each major application and disseminate information among institutions.
29. Workshops, training, education on terms of service.
30. Executive training/digital literacy - get CIOs involved.

Educating our students:

31. Ask students if they want academic "social media" incorporated in their private social media life.
32. Educate students about digital privacy. Education is key: what about making a course - just like getting a drivers' exam? We need to ensure we are educating about the risk.
33. Start at K-12 level through into post-secondary.
34. This is ethical issue too, and we need to touch in this in education for IT degrees, communication degrees, marketing, education, etc.