BCcampus and Identity Management

Anonymizing Authorized Student Access to Services Hosted in Foreign Domains

A Potential Federated Identification Management Solution

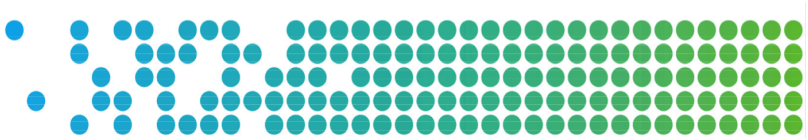
April 19, 2011

Revision History

Date	Author	Comments
April 19, 2011	Anthony M. Patrick	Initial version of this document
June 8, 2011	Randy Bruce	Changed title, applied BCcampus template

Contents

200-555 Seymour St
Vancouver BC V6B 3H6
Tel 604.412.7657 | Fax 604.677.6273
www.bccampus.ca



1 Reason for this Analysis/Potential Initiative

Although the " Freedom of Information and Protection of Privacy Act" of British Columbia prohibits the unauthorized collection, use or disclosure of personal information by public bodies; post-secondary students within the province are being encouraged to "join" online communities and make use of computerized systems which are not within the jurisdiction of the province. The computers hosting the majority of these communities are subject to the American "Patriot" act. For example:

- Social networking sites (eg. Facebook, Twitter, Flickr, You Tube, etc.) are being used by students in pursuit of their academic and career goals. The social networking sites have become a preferred conduit for information interchange amongst students relating to course work. The use of social networking sites for these purposes are often encouraged by faculty who are teaching the courses. Unfortunately, the majority of the social networking sites are hosted on computers either located in the United States of America or on computers owned and operated by subsidiaries of American companies. As such, the data recorded on these computers is subject to the American "Patriot" act. Hence personal and private data (names, addresses, identifiers, and personal logs) recorded on these computers are subject to scrutiny by the American government and as such the privacy of the student may be violated.

- Students use networking sites such as "Survey Monkey", "Survey Gizmo", "Kwik Surveys", etc. to create "surveys" and solicit participation from other students. Again, the computers hosting the majority of the "survey" engines are subject to the American "Patriot" act.

- Students are asked to participate in surveys relating to the delivery of services by the post-secondary institutions which they are attending. These surveys range from questions relating to the quality of education, questions relating to the quality of campus life, questions relating to the delivery of health-care on campus, etc. The results of these surveys are widely published and used by prospective students in selecting teaching institutions and courses. Again, the computers hosting the majority of the "survey" engines are subject to the American "Patriot" act or on computers that are not within the jurisdiction of the province.

All of these social networking sites / survey sites require individuals to identify themselves in some way before access is allowed. This identification can include name, gender, birth-date, and e-mail address (look at the "facebook" registration page as an example). The veracity of the self-reported identification is normally not checked in the identification / registration process for these sites - it is simply recorded and used as a backup to the sign-on credentials assigned by these sites. Often, the e-mail address is used as a "proxy" for a login identifier. Regardless, this information is being collected!

200-555 Seymour St
Vancouver BC V6B 3H6
Tel 604.412.7657 | Fax 604.677.6273
www.bccampus.ca

2 Service Concepts

There are three options for minimizing the recording of personal / private information on computers that are outside the jurisdiction of the privacy legislation of the province:

1. Host an equivalent service on a computer administered by a public body (such as BCcampus) within the province that is subject to the privacy legislation. Use of a "federated identification" login capability (such as Shibboleth) would insure privacy.

2. Where the first option is not viable, negotiate a "trust relationship" with each social networking site provider whereby the login credentials of the individual requesting access to the service are made available through an intermediary (such as BCcampus). In this way personal / private information is guaranteed not to released to the provider. This is core to what a "federated identification" login capability (such as Shibboleth) provides.

3. Where the first two options are not viable, "anonymize" the identification of the student with an easy-to-use mechanism by providing a front-end interface to the desired service(s) and by using a "federated identification" login capability (such as Shibboleth) to insure privacy.

2.1 Hosting an Equivalent Service

The most obvious solution to the privacy problem is to provide an equivalent service hosted on a computer that is governed by the privacy legislation. However this solution is problematic because of three compelling factors:

a) The equivalent service may not be acceptable or accepted. The online communities (especially the social networking communities) thrive on having a very large number of members who are not restricted by jurisdiction or political borders. A "local" version of something like "Facebook" for BC students only would not be well accepted.
b) The software development costs and operating costs for these types of applications are staggering.
c) There are intellectual property issues / risks when attempting to engineer an "equivalent" service.

However there is one case where hosting an equivalent service could work well. That is the case of "surveys" that are created by students as part of their course work. These types of surveys tend to be "local" in nature and the people to be surveyed are often other students in the same community. The identification of the survey creator and the data collected from survey participants can be at risk. There are "open source" solutions such as "LimeSurvey" whereby the survey software can be freely downloaded and hosted on computers that are subject to the privacy legislation of the province. The software, being open source, is risk free in regards to intellectual property rights and can be embellished to allow for a "federated identification" login capability to insure privacy.

200-555 Seymour St
Vancouver BC V6B 3H6
Tel 604.412.7657 | Fax 604.677.6273
www.bccampus.ca

2.2 Negotiating a "trust relationship"

Unfortunately none of the large social networking sites accept "trust relationship" credentials. Although technologies (such as Shibboleth) exist for providing access to the site via an intermediary (such as BCcampus) in such a way that personal / private information is not released to the provider; the large social networking sites have not implemented this (yet?).

At this point, the best plan of action is to lobby the social networking site providers whenever the opportunity presents itself to implement "federated identification" login capability.

2.3 "Anonymizing" the Student's Identification

Because the veracity of the self-reported identification is normally not checked in the identification / registration process for most of the social networking sites; it would be possible to "anonymize" student access by creating pseudonyms when accessing these sites. The same is true for the survey sites that require individuals to identify themselves in some way before access is allowed. (SFU has successfully implemented an "anonymizing" student interface to the NIH sponsored health survey that is used to gather statistical data relating to health care on campuses in North America.)

The anonymizing mechanism would work something like this:

1. The student directly creates a pseudonym (or potentially receives a pseudonym from a central source) for access to a social networking site (or a survey site).
2. The pseudonym for the social networking site is registered to the student in a central site (such as BCcampus) which is subject to the privacy legislation of the province. A "federated identification" login (such as Shibboleth) on a BCcampus hosted service could be used as the registration vehicle. BCcampus maintains the cross-reference between the student's pseudonym and the federated login identifier. The student's home institution maintains the cross-reference between the federated login identifier and the actual student's identification. In this way, the privacy of the student is preserved.
3. The student accesses the social networking site either by directly using his/her pseudonym or by using a front-end WEB interface hosted by BCcampus (the cross-reference repository site).
4. Should the educational institution need to check that the student has indeed completed his/her coursework as intended, the cross-reference links could be used (subject to privacy legislation) to backtrack.

200-555 Seymour St
Vancouver BC V6B 3H6
Tel 604.412.7657 | Fax 604.677.6273
www.bccampus.ca

3 Enabling Computer Technologies

1. "Federated identification" login technologies hosted on computers subject to the privacy legislation of the province are at the core of the proposed services.
2. Database technologies are needed to record the cross-references between student pseudonyms and the federated login identifier.
3. Web services technologies needed to provide an easy-to-use "front-end" for accessing social networking sites / survey sites using pseudonyms. (However this technique may not be possible in all cases in which case a student would need to directly input his/her pseudonym.)

It is important to note that these technologies should be hosted by public bodies who are subject to the privacy legislation of the province. This helps insure that the privacy of the students will be enforced in spirit as well as by legislation.

200-555 Seymour St
Vancouver BC V6B 3H6
Tel 604.412.7657 | Fax 604.677.6273
www.bccampus.ca

4 A Potential Path Forward

1. The enabling technologies would be hosted on computers that are subject to the privacy legislation of the province. BCcampus is an obvious choice as a provider because this is the organization already charged to foster educational technology and distance learning for BC's public post-secondary institutes and is itself subject to the privacy legislation of the province.

2. Because "Shibboleth" technology is being used by the large universities within the province for providing "federated login" identification and because this technology has also been implemented by BCcampus, it too is an obvious choice. This does not preclude adding additional federated identification technologies at a later date if the requirements present themselves.

3. Each participating educational institution within the province would need to provision a "Shibboleth" Identity Provider service (Idp) which would interact with the central student pseudonym cross-reference service. (Computer servers that are already provisioned by BCcampus to the post secondary institutions could be embellished with this software technology.)

4. BCcampus would implement the pseudonym cross-referencing service as described in this paper.

5. BCcampus would review and potentially implement survey software (such as "LimeSurvey") to address the issue of "surveys" created by students as part of their course work.

200-555 Seymour St
Vancouver BC V6B 3H6
Tel 604.412.7657 | Fax 604.677.6273
www.bccampus.ca