THE Research Universities' Council OF BRITISH COLUMBIA

January 29, 2016

Don McRae, MLA
Chair, Special Committee to Review the *Freedom of Information and Protection of Privacy Act*
c/o Parliamentary Committees Office
Room 224, Parliament Buildings
Victoria, BC V8V 1X4

Dear. Mr. McRae,

On behalf of the members of The Research Universities' Council of British Columbia (RUCBC), thank you for the opportunity to provide input on the effectiveness of the *Freedom of Information and Protection of Privacy Act (FIPPA)*.

RUCBC represents and provides a common voice for its members - The University of British Columbia, Simon Fraser University, University of Victoria, University of Northern British Columbia, Royal Roads University and Thompson Rivers University – on public policy issues including funding, accountability, research and post-secondary education.

RUCBC member institutions take freedom of information and protection of privacy very seriously and welcome this opportunity to provide comment. Although we have broad interest in FIPPA, the submission focuses on the prohibition in section 30.1 against storage of personal information outside of Canada. This section affects a number of key areas of university business and the research universities' ability to meet their commitments to students, Government and British Columbians.

Specifically, Section 30.1 of the FIPPA has significant implications for the following:

- Administrative efficiency and security
- International engagement and student recruitment
- Online learning offerings
- Academic integrity

… /2.

The attached submission describes these challenges, suggests potential solutions and proposes amendments for consideration by the Special Committee. If further information is required, we would be pleased to provide it to you or to the Special Committee.

Thank you for your consideration and we look forward to the results of the Special Committee's review in the report due later this year.

Yours truly,

Robin Ciceri
President

copy: Hon. Amrik Virk, Minister of Technology, Innovation and Citizens' Services
Hon. Andrew Wilkinson, Minister of Advanced Education
Sandra Carroll, Deputy Minister of Advanced Education
Bette-Jo Hughes, Associate Deputy Minister and Chief Information Officer
Martha Piper, Interim President, The University of British Columbia
Andrew Petter, President, Simon Fraser University
Jamie Cassels, President, University of Victoria
Daniel J. Weeks, President, University of Northern British Columbia
Allan Cahoon, President, Royal Roads University
Alan Shaver, President, Thompson Rivers University

The Research Universities' Council of British Columbia

SUBMISSION TO THE SPECIAL COMMITTEE TO REVIEW THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Introduction

The Research Universities' Council of British Columbia (RUCBC) works with and on behalf of the six major universities − UBC, SFU, UVic, UNBC, RRU, and TRU − to improve the quality, accessibility and coordination of university education in British Columbia. The Council provides its members with a single voice with respect to public policy issues including funding, research, accountability, admissions and transfer.

The recommendation contained in this submission reflects the consensus view of the members of RUCBC with respect to the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). We also believe that these recommendations have broad support within the post-secondary education sector.

While post-secondary institutions have several comments about the FIPPA, we have chosen to focus this submission on the prohibition in section 30.1 against storage of personal information outside of Canada. No section of the FIPPA has caused greater difficulties for our sector.

Impacts of Section 30.1

Under section 30.1 of the FIPPA, public bodies and their service providers are prohibited, under most circumstances, from disclosing and storing personal information outside of Canada. British Columbia is one of only two jurisdictions in Canada that imposes this restriction. (The other jurisdiction is Nova Scotia, but that province is much less restrictive because it allows public bodies to make exceptions "if the head considers the storage or access is to meet the necessary requirements of the public body's operation").

As the world moves towards vendor hosted or "cloud computing" solutions, in our opinion the prohibition contained in section 30.1 of the FIPPA is putting universities at a disadvantage because we are prevented from using the same world-class tools that are used elsewhere. Despite the reality that these new solutions are often more expensive than traditional IT solutions, vendors are limiting the availability of choice to cloud services only. Here are a few examples of the impacts we are already experiencing:

Impact on administrative efficiency and security: Educational bodies, like many other organizations, depend on specialized enterprise resource planning (ERP) services to store and process HR, payroll, and student information. The major vendors of ERP services are planning a shift to the cloud over the next several years. Some vendors have informed us that on-premise services will not be available. Without changes, the current section 30.1 restrictions will prevent institutions from continuing to use these services. Our CIOs inform us that competitive alternatives for many of these systems are not available in Canada.

Impact on international engagement and recruitment: Some BC universities operate international offices for purposes such as student recruitment, exchange, development and career support; alumni engagement and support; fund-raising; and academic and research activities. Section 30.1 prevents

university employees who work in these offices from accessing university systems containing personal information, such as student information systems. This makes it virtually impossible for these offices to operate in an effective manner.

Impact on online learning: Universities across Canada and around the world are increasingly using sophisticated learning management systems to deliver electronic courses to their students. Many of these systems are designed to be seamlessly integrated with online learning, study and testing tools for students. However, British Columbia universities are not permitted to allow their students to use these tools, because of section 30.1. Thus students in this province are being deprived of learning opportunities that are available to their counterparts throughout the world.

Impact on academic integrity: Online plagiarism detection services, such as Turnitin.com, are used by many educational institutions in North America. The software is designed to seamlessly integrate with the learning management systems used by universities, but BC institutions have had to disable this integration because the service would have access to student names from outside Canada. The inability to efficiently use these services has made it more difficult for instructors to ensure the integrity of their educational programs.

These are only a few examples of the impact of section 30.1 upon the ability of BC post-secondary institutions to compete with institutions across Canada and around the world. This section has not appreciably enhanced the security of personal information.

We do not disagree with the goal of section 30.1 to protect the personal information of British Columbians from access by foreign intelligence and law enforcement agencies. In particular, the USA PATRIOT Act and the National Security Agency's mass electronic surveillance program have raised legitimate concerns about the confidentiality of personal information stored in the United States.

However, there are more effective ways to address these concerns other than by creating a near-absolute prohibition against storage or access to personal information outside of Canada. Other privacy regimes typically recognize the principle of proportionality: efforts to ensure security must be proportional to the risk of unauthorized disclosure. Factors such as the type(s), sensitivity and volume of the personal information involved must be considered. Section 30.1 contains no proportionality test; it applies to virtually all personal information, even if the information is of a low degree of sensitivity or is protected with state-of–the-art security features such as encryption.

While section 30.1(a) authorizes the disclosure of personal information outside Canada with the consent of the individual, securing consent is not always a viable option. As "forced consent" is an oxymoron, a valid consent process must provide a reasonable alternative for those who do not want to consent. However, designing a reasonable alternative for many of the specialized systems used by universities is effectively impossible. For example, an instructor who wants her students to use an online learning tool may not be able to design an alternative for those who choose to opt out. The result is that a single student who withholds consent may prevent the use of the tool by their entire class.

A robust privacy impact assessment (PIA) process will capture the proportionality test and apply it to the specific proposed system. We propose that the PIA for any system that allows foreign storage or access of personal information will be shared with the Office of the Information and Privacy Commissioner for its review and comment. Without the test of proportionality, section 30.1 remains a blunt instrument, which we are unable to demonstrate has significant public benefit.

In addition to the usual limits to the storage of personal information and the robust PIA process, we propose storage or access outside of Canada be permitted only where:

a) the storage/access relates directly to and is necessary for a program or activity of the public body;
b) there is no reasonable Canadian-based alternative available;
c) security measures are in place to protect the personal information, that are proportional to the risk posed based upon an analysis of the type(s), sensitivity and volume of the personal information; and
d) it is impractical to obtain consent.

For the above reasons, universities are seeking amendments to section 30.1. Public bodies should be allowed to store or allow access to personal information outside Canada when it has determined that they meet the above criteria. Any storage or access to personal data outside Canada would, of course, be subject to the oversight of the Information and Privacy Commissioner. These amendments will facilitate the delivery of the highest quality public services while maintaining British Columbia's position as a world leader in personal information protection.

Recommendation

We recommend that sections 30.1(c) and 33.1(1) be amended to expressly authorize public bodies to store and disclose personal information outside Canada only when the head has determined that (a) this relates directly to and is necessary for a program or activity of the public body; (b) a reasonable Canadian-based alternative is not available; (c) security measures, proportional to the risk posed by the type(s), sensitivity and volume of personal information are in place to protect the data; and (d) it is impractical to obtain consent. Section 69 should also be amended with a requirement to share the privacy impact assessment for the project with the Office of the Information and Privacy Commissioner for its review and comment.