a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

Office of the University Counsel
Legal Counsel, Information and Privacy
6328 Memorial Road
Vancouver, BC Canada V6T 1Z2

Phone 604 822 2451
Fax 604 822 8731
access.and.privacy@ubc.ca

Privacy Fact Sheet

Disclosing Personal Information Outside Canada

Introduction

1. Public bodies in British Columbia, including UBC, are subject to restrictions on the storage or access to personal information from outside Canada. These restrictions, which are contained in the *Freedom of Information and Protection of Privacy Act* (FIPPA), require all personal information in UBC's custody or control to be stored only in Canada and accessed only in Canada, with a few narrowly defined exceptions.[1] The Office of the University Counsel has developed this Privacy Fact Sheet to explore the implications of these restrictions for UBC faculty and staff members.

2. This Privacy Fact Sheet is not a substitute for legal advice. If you have questions about a specific situation, contact the Legal Counsel, Information and Privacy in the Office of the University Counsel.

Implications for Cloud Services

3. Many computing services are offered through the Internet, and may be hosted in the United States or other foreign jurisdictions. Using these services to collect, store, transmit or access personal information is a violation of the restrictions against storage or access outside Canada.

4. Here are some examples of commonly used cloud services, with Canadian-based alternatives:

Cloud Services	Canadian-based Alternatives
Dropbox	Workspace
Gmail, Hotmail	FASmail
Survey Monkey	Fluid Surveys (UBC IT version)
Google Docs	Microsoft Word and Excel

5. If a Canadian-based alternative does not exist, you may nevertheless be authorized to use the service if it falls under one of the exceptions listed below.

[1] Section 30.1 of the FIPPA

Exceptions

6. The FIPPA allows storage or access to personal information outside Canada in several situations, among which are the following:

Consent

7. It is acceptable to store or access an individual's personal information outside Canada if you have the consent of the individual. This consent must be in writing and must specify:

    a. who may store or access the personal information;
    b. if practicable, the jurisdiction in which the personal information may be stored or from which the personal information may be accessed; and
    c. the purpose of the storage of or access to the personal information.

8. As a forced consent is not valid, you need to have an alternative in place for those individuals who choose not to provide their consent.

9. Instructors often use cloud services hosted outside Canada in their courses. If these services involve the collection of student name, contact information, or other personal information, then the instructors need to seek the students' consent to use these services. Since it may not be practical to secure written consent from every student, it is acceptable for the instructor to secure the consent as follows:

    a. in the course description, or in a written communication to the students, describe the cloud-based service and the information that it will be storing or accessing, and explain that if the students choose not to provide their consent to this storage or access, they must see the instructor to make alternate arrangements; and
    b. make alternate arrangements for students who refuse to provide their consent, such as allowing them to sign in to the service using a false name and non-identifying email address.

Sample Communication about Cloud-Based Services

In this course, students will be required to use Piazza, an online collaborative service. During the account creation process, Piazza will collect your name and other identifying information. By using Piazza, you are consenting to the storage of this information in the United States. If you choose not to provide your consent, see the instructor to make alternate arrangements.

Employees Travelling Outside Canada

10. The FIPPA allows faculty and staff members who are temporarily travelling outside Canada to store personal information or access this information remotely on UBC systems.[2] This exception in limited to employees who are temporarily travelling; it does not apply to employees who are living overseas.

[2] Section 33.1(e.1) of the FIPPA

Receiving Payments

11. The FIPPA allows personal information to be stored or accessed outside Canada for purposes related to a payment to be made to UBC.[3] These purposes include authorizing, administering, processing, verifying or canceling such a payment, or resolving an issue regarding the payment.

12. This exception allows UBC to use credit card and other payment services that store personal information outside Canada.

Research

13. Personal information may be stored or accessed outside Canada for a research purpose, provided the recipient has signed a research agreement with UBC and various other privacy and security conditions have been approved.[4] For more information, speak to the Legal Counsel, Information and Privacy.

Installation, Maintenance and Repair of Electronic Systems

14. Temporary access or storage of Personal Information outside of Canada is acceptable, provided that this is:

    a. necessary for installing, implementing, maintaining, repairing, trouble-shooting or upgrading an electronic system or recovering data from such a system; and
    b. limited to the minimum amount of time necessary for that purpose.[5]

[3] Section 33.1(i.1) of the FIPPA
[4] Section 33.1(s) and 35(1) of the FIPPA
[5] Section 33.1(p) of the FIPPA