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

Overview of Privacy

Introduction

1. A classic definition of "privacy" is "the right to be left alone." Privacy encompasses the freedom from intrusions into one's physical space, and the right to control disclosure of one's private information. For UBC's purposes, however, "privacy" can best be defined as a set of rules governing the collection, use, disclosure, protection, storage and retention of personal information.

2. The privacy rules applicable to UBC are set out in the *Freedom of Information and Protection of Privacy Act* (FIPPA). The purpose of this Fact Sheet is to summarize the privacy-related requirements of the FIPPA at a high level for the benefit of UBC staff and faculty members. It is not intended to be a substitute for legal advice. Additional Fact Sheets and other resources are available that explore in greater depth how the FIPPA applies in specific circumstances. Also, the Legal Counsel, Information and Privacy in the Office of the University Counsel is available to answer privacy-related questions.

Privacy Laws in British Columbia

3. UBC is subject to the FIPPA, which is one of several privacy laws that apply in British Columbia. The following chart shows these laws and examples of organizations that are subject to them.

	Public Sector Organizations	**Private Sector Organizations**
Provincial Jurisdiction	**Applicable Law:** *Freedom of Information and Protection of Privacy Act* (FIPPA) **Examples:** UBC; BC Ministry of Finance; ICBC; City of Vancouver	**Applicable Law:** *Personal Information Protection Act* (PIPA) **Examples:** Alma Mater Society; CUPE; Tim Horton's
Federal Jurisdiction	**Applicable Law:** federal *Privacy Act* **Examples:** Canada Revenue Agency; RCMP; Canada Post	**Applicable Law:** *Personal Information Protection and Electronic Documents Act* (PIPEDA) **Examples:** Telus; Royal Bank; WestJet

4. In addition to the above laws, BC also has a *Privacy Act* (which should not be confused with the federal *Privacy Act*). The BC *Privacy Act* gives individuals the right to sue others, and receive damages, for:

    a. willfully violating their privacy[1]; or
    b. using their name or portrait for the purpose of advertising property or services, without that person's consent.[2]

Overseeing Compliance with the FIPPA

5. UBC's Board of Governors has delegated to the University Counsel the overall responsibility to ensure that UBC complies with the FIPPA. The Legal Counsel, Information and Privacy, reporting to the University Counsel, administers these responsibilities on a day-to-day basis.

Application of the FIPPA

6. The FIPPA regulates the activities of the following individuals at UBC:

    a. employees, including staff and faculty members;
    b. volunteers; and
    c. employees, officers, directors, affiliates, and subcontractors of service providers (ie. persons or corporate entities retained under a contract to perform services for UBC).

7. The FIPPA does not regulate the activities of students, unless they are acting as employees, volunteers or service providers of UBC.

8. The FIPPA does not apply to independently incorporated entities that are associated with UBC, such as the Alma Mater Society and Alumni Association.

What Privacy Rights do Individuals Have?

9. Under the FIPPA, individuals have the right to expect public bodies to collect, use, disclose, retain and protect their personal information in a lawful and appropriate manner. They also have the right to:

    a. access their own personal information;
    b. request correction of their own personal information if they believe it is inaccurate;
    c. consent to the collection, use and disclosure of their own personal information; and
    d. complain to the Information and Privacy Commissioner if they believe their privacy has been breached.

10. Only private individuals have a right to privacy. Companies and other organizations do not have privacy rights.

---

[1] Section 1(1) of the BC *Privacy Act*
[2] Section 3(2) of the BC *Privacy Act*

11. Under some circumstances, an individual's privacy rights may be exercised by somebody else if he or she is under the age of 19, physically or mentally unfit, or deceased. For more information, refer to the Fact Sheet "Minors, Mentally Incapable and Deceased Individuals".

What is Personal Information?

12. "Personal information" comprises **all recorded information about an identifiable individual, with the exception of the names and business contact information of employees, volunteers and service providers**.

13. The FIPPA does not distinguish between different types of personal information. The terms "personally identifiable information" (PII) or "protected health information" (PHI) are not used in the FIPPA.

14. Personal information must have a precise, direct connection with one identifiable individual. For more information, refer to the Fact Sheet "What is Personal Information?"

Is an Address Personal Information?

- "123 Main Street" is **not** personal information (because it can't, by itself, be linked to an identifiable individual)
- "Jane Doe works at 123 Main Street" is **not** Jane's personal information (because it is her business contact information)
- "Jane Doe lives at 123 Main Street" **is** Jane's personal information

Collecting Personal Information

15. The FIPPA lists several circumstances under which personal information may be collected.[3] For example, section 26(c) of the FIPPA authorizes us to collect information if it "relates directly to and is necessary for an operating program or activity" of UBC.

16. Generally, personal information must be collected with the individual's knowledge. Covert collection of personal information (eg. surveillance by hidden cameras) is only permissible in exceptional circumstances, and requires the written authorization of the Legal Counsel, Information and Privacy.

17. Also, personal information must usually be collected directly from the individual it is about. Indirect collection of personal information is only authorized under limited circumstances.[4]

18. When you collect someone's personal information, you must generally give that individual a "privacy notification" stating UBC's legal authority to collect the information, how the information will be used, and the contact information of somebody who can answer questions about the collection. [5]

"Direct" vs. "Indirect" Collection:

- If you ask John for his home address, you are **directly** collecting his personal information. **This is the recommended method of collection**.
- If you ask John's friend Mary for John's home address, you are **indirectly** collecting information about John. **In most circumstances, this method of collection is not authorized.**

[3] Section 27(1)(c) of the FIPPA
[4] Section 27 of the FIPPA
[5] Section 27(2) of the FIPPA

19. For more information about when and how to collect personal information, see the Fact Sheet "Collecting Personal Information".

Using Personal Information

20. Generally, you are only authorized to use personal information for the purpose for which it was obtained or compiled or for a use consistent with that purpose.[6] Therefore, it is essential for you to know the purpose for which UBC obtained the data. This purpose is usually stated in the "privacy notification" that we give to individuals when we collect their information.

Example of "Consistent Use":

The UBC Student Health Service collects medical information from students for purposes related to the students' medical care. It would not be consistent with this purpose to use this information for fundraising purposes.

21. Many IT systems provide the ability to store large amounts of personal information in centralized data repositories. When personal information collected for different purposes is mixed together in a single system, it becomes more likely that the purposes for collection will be forgotten and the data will be used inappropriately. Where possible, therefore, databases of personal information should only be linked when they were collected for a consistent purpose.

Disclosing Personal Information

22. The FIPPA contains a long list of circumstances under which we are authorized to disclose personal information.[7] The Office of the University Counsel has issued Fact Sheets that explain some of the most common circumstances, including: "Disclosing Personal Information to Law Enforcement Agencies and Government Bodies"; "Disclosing Personal Information for Health and Safety Reasons" and "Disclosing Personal Information Outside Canada".

23. Generally speaking, personal information may be disclosed in two ways:

    Internal disclosure: This is disclosure of personal information to other UBC employees, volunteers or service providers. As a rule, internal disclosure is permitted on a "need-to-know" basis.[8]

    External disclosure: This is disclosure of personal information to somebody outside UBC. External disclosure is tightly restricted and generally requires the written consent of the individual who the information is about, or authorization from the Legal Counsel, Information and Privacy.

Internal vs. External Disclosure

- UBC Financial Services staff may need to share students' financial information with each other for the purpose of processing student loan requests. This is **internal disclosure** within UBC and is permitted on a "need-to-know" basis.
- UBC staff may also receive questions about students' financial situations from the students' parents or legal representatives. This is **external disclosure**, which usually requires the student's written consent.

[6] Section 32(a) of the FIPPA
[7] Section 33 of the FIPPA
[8] Section 33.1(e) of the FIPPA

Protecting Personal Information

24. Under the FIPPA, we are required to protect personal information by "making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal".[9] UBC requires individual units to ensure that the appropriate security measures are observed for records containing personal or other confidential information.[10]

25. For an overview of requirements governing the security of personal information, refer to the UBC Information Security Standards.

26. Many privacy protection issues arise out of the use of information technology because the ability to store large amounts of data on personal computers and other devices has significantly increased the risk of serious privacy breaches. UBC's IT Security Office has published resources that explain how to protect information on these devices.

27. Outsourcing data storage and analysis to specialized service providers may also have a significant impact upon security and privacy. UBC remains ultimately responsible for the security of data we outsource, so we are obliged to ensure that our service providers have the appropriate safeguards in place to protect this data. Usually, we require service providers to sign a System Access and Confidentiality Agreement, which sets out their privacy obligations in detail.

Storing Personal Information Outside Canada

28. The FIPPA contains special restrictions on the disclosure of personal information outside Canada. Generally, UBC cannot allow personal information to be stored or accessed outside Canada without the written consent of the individual the personal information is about.[11] This limits our ability to use "cloud computing" services or to outsource data storage or processing services outside Canada.

29. For more information about restrictions on disclosing personal information outside Canada, refer to the Fact Sheet "Disclosing Personal Information Outside Canada".

Examples of "Cloud Computing":

Facebook, SurveyMonkey, Dropbox and Hotmail are just a few examples of "cloud computing" services that should generally not be used to collect or disclose personal information because they store this information outside Canada.

Retaining Personal Information

30. Retention periods must be established and followed for all records, including records containing personal information. All records must be retained for as long as they are required to meet legal, administrative,

[9] Section 30 of the FIPPA
[10] Section 2.4 of Policy No. 117, Records Management
[11] Section 30.1 of the FIPPA

operational, and other requirements of the University.[12] The University Archives should be consulted for advice about establishing appropriate retention periods.

31. The FIPPA requires UBC to retain personal information for a minimum of one year after it is used to make a decision that directly affects the individual.[13] The purpose of this "privacy retention" requirement is to give the individual a reasonable opportunity to obtain access to his or her personal information.

Privacy Retention Example:

A manager has just hired an employee. All the resumes and other personal information she reviewed during the hiring process must be retained for at least one year.

32. While the FIPPA does not impose a maximum retention period for personal information, it is considered good practice not to retain personal information longer than necessary. Therefore, the growing tendency to store data permanently (on the principle that it is cheaper to do so than to selectively delete data) is often inconsistent with good privacy practices.

33. The University Records Manager can provide more guidance about records retention.

Ensuring Accuracy and Completeness of Personal Information

34. An individual who believes there is an error or omission in his or her personal information may request the information to be corrected.[14] If UBC does not make a correction, it must annotate the information with the correction that was requested but not made. All requests for correction of personal information should be referred to the Legal Counsel, Information and Privacy.

Conducting Privacy Impact Assessments

35. New systems, projects, programs and activities, and agreements with service providers may all have an impact upon privacy. The process used to evaluate these privacy implications is called a Privacy Impact Assessment (PIA). Under the FIPPA, UBC is obliged to conduct PIAs and, in some cases, is required to submit them to the Information and Privacy Commissioner for review and comment.[15]

36. PIAs must be reviewed and approved by the Legal Counsel, Information and Privacy.

37. For more information about how to conduct a PIA, refer to the instructions on the University Counsel website.

[12] Section 2.2 of Policy No. 117: Records Management
[13] Section 31 of the FIPPA
[14] Section 29 of the FIPPA
[15] Sections 69(5.3) and 69(5.4) of the FIPPA

Dealing with Privacy Breaches

38. Privacy breaches occur when there is unauthorized access, collection, use, disclosure or disposal of personal information. Privacy breaches may cause significant harm to affected individuals and may also constitute an offence under the FIPPA.[16]

39. You are required to notify the Legal Counsel, Information and Privacy if you have reason to believe that there has been a privacy breach.[17] For more information about how to deal with a privacy breach, refer to the Fact Sheet "Handling Privacy Breaches".

[16] Section 30.4 and 74.1 of the FIPPA
[17] Section 30.5 of the FIPPA