Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

CLOUD COMPUTING GUIDELINES FOR PUBLIC BODIES

UPDATED JUNE 2012

Purpose

Increasingly, public bodies in British Columbia are exploring ways to take advantage of the cost-savings and functionality presented by a type of service often called "cloud computing". Cloud computing has been described as follows:

> The rise of "cloud computing"––the practice of using the Internet to process, manage and store data on remote network services––now permits individuals to perform traditionally private activities on the Internet. This computing trend is fuelling a mass migration of information, once stored on the hard drives of personal computers, to remote servers in a domain controlled by online service providers.[1]

Examples of cloud computing include web-based email, social networking sites and document collaboration tools. In these guidelines, storage of information "in the cloud" refers to the use of cloud computing by any of these means.

The purpose of this resource is to provide information to public bodies about how BC's *Freedom of Information and Protection of Privacy Act* ("FIPPA")[2] applies.

---

[1] Nied, "Cloud Computing, the Internet, and the *Charter* Right to Privacy: The Effect of Terms of Service Agreements on Reasonable Expectations of Privacy" (2011), 69 *The Advocate* 701 at 706.

[2] FIPPA is available online at: www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00.

Three Key Terms

FIPPA applies to *personal information* that is *in the custody or under the control of* a *public body*. Understanding what these terms mean is essential to understanding how FIPPA applies to the cloud.

What is "*personal information*"? Why is this important?

The term "personal information" is defined in FIPPA and means any recorded information about an identifiable individual.[3] For example, if a student emails her teacher about her parents' divorce, that email contains recorded information about the student *and* her parents. If the student and her parents are identifiable from the email (whether they are named or not), then that information is personal information. It is important to understand what personal information is because FIPPA sets out requirements about protecting, storing and accessing it.

What is "*in the custody or under the control of*"? Why is this important?

Unlike other terms in FIPPA, the words "custody" and "control" are not defined. Determining who has custody or control of personal information can be challenging and depends on a variety of circumstances.[4] FIPPA only applies to personal information that is "in the custody or under the control of" a public body. For example, if while working, a librarian posts photos of his vacation on his social networking profile, it is unlikely those photos would be considered to be "in the custody or under the control of" the library. By contrast, if the librarian posts photos of people reading magazines in the library on the library's social networking page, it is likely those photos would be considered to be in the custody or under the control of the library.

It is important to understand this concept for two reasons: First, FIPPA sets out specific requirements detailing how public bodies must manage this information. Second, FIPPA provides a right for anyone to make a request for access to records containing that information.

---

[3] "Personal information" excludes "contact information", defined as "information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual": FIPPA, Schedule 1.

[4] For a non-exhaustive list of some of the other factors of whether a public body has custody or control of personal information contained in a record, see Order F06-01, [2006] B.C.I.P.C.D. No. 2; online at www.canlii.org/en/bc/bcipc/doc/2006/2006canlii3255/2006canlii3255.html, at para. 81.

What is a "*public body*"? Why is this important?

There are more than 2,900 public bodies in BC. The term "public body" is defined in FIPPA and includes schools, hospitals, municipalities, and more. It is important to determine whether your entity is a public body because of the rules about what public bodies can do with personal information.

In summary, if a public body has personal information that is in its custody or under its control, it must comply with FIPPA. This includes employees as well as volunteers and service providers, as they are included in the definition of "employee" provided in FIPPA.

What the Law Says

Storing and accessing personal information ***outside of Canada***

In addition to the requirement for public bodies to protect personal information no matter where it is, FIPPA also requires public bodies to ensure that, subject to three exceptions listed in s. 30.1 of FIPPA, personal information is only stored in and accessed from inside Canada.[5] This presents an issue for public bodies because currently, many companies that offer cloud computing store information outside of Canada.

Public bodies must consider s. 30.1 of FIPPA when making decisions about whether to store personal information in the cloud. With limited exceptions as set out in FIPPA, personal information, including information in computer logs and on backup tapes or drives cannot be stored or accessed outside of Canada. Under FIPPA, it is an offence to store or allow access to personal information outside of Canada unless it is authorized.[6]

---

[5] In 2009 the BC Government made a submission to a special committee of the Legislative Assembly that the prohibition on storage and access outside of Canada should change. The Committee's subsequent report did not endorse this recommendation but it acknowledged the challenges public bodies face as a result of this requirement. Complete information about the Committee, its report and all submissions received are available online at www.leg.bc.ca/foi/.

[6] See FIPPA, s. 74.1(2)(a).

Consent *to store or access personal information outside of Canada*

Under s. 30.1(a) of FIPPA, public bodies can store or access personal information outside of Canada if the individual the personal information is about has given consent to the public body to do so. The consent must be in the prescribed manner. The regulations to FIPPA[7] set out the requirements for consent under s. 30.1(a). According to the regulations, an individual's consent must be in writing and must specify the personal information for which the individual is providing consent, the date on which the consent is effective and, if applicable, what date the individual's consent expires. The consent must also specify who may store or access the personal information from outside of Canada, and if it is practicable, which jurisdiction the personal information may be stored in or accessed from. The consent must also specify the purpose of storing or accessing the personal information.

One challenge with consent is that recorded information often contains the personal information of multiple individuals. For example, if a public body wanted consent to store a student's email about her parents' divorce on a server located outside of Canada, the public body would have to obtain the consent of both the student and each of her parents. If the student's next email contained the personal information of the friends she made during spring break, the public body would have to get their consent too.

Other *exceptions to the rule about storing and accessing personal information*

Under ss. 30.1(b) and (c), other exceptions apply. In s. 30.1(b), personal information may lawfully be stored in another jurisdiction "for the purpose of disclosure allowed under this Act".[8] In s. 30.1(c), personal information may lawfully be stored in another jurisdiction if it was disclosed in relation to monetary payments to be made by or to the government.[9]

Protecting *personal information*

Whether a public body stores personal information in its own offices, across the street or throughout the world, all public bodies are legally required under FIPPA to

---

[7] Freedom of Information and Protection of Privacy Regulation, s. 11. The FIPPA regulations are online at www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/11_323_93.

[8] One example of this would be storage of personal information in another jurisdiction under a treaty: see s. 33.1(1)(d) of FIPPA. Another would be where the Minister responsible for FIPPA has issued an order to allow disclosure of personal information outside of Canada in circumstances where disclosure is normally authorized only inside Canada: See s. 33.1(3) of FIPPA. Copies of Ministerial Orders under s. 33.1(3) allowing disclosure of personal information outside of Canada are available online at: www.cio.gov.bc.ca/cio/priv_leg/foippa/order_summaries/min_orders.page.

[9] See s. 33.1(1)(i)(i)) of FIPPA.

protect that information. The standard in FIPPA is that public bodies must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

Reasonable security arrangements in the context of cloud computing will usually require a public body to review the security that the cloud provider has in place. Key areas should be reviewed and considered from the perspective of reasonable security, taking into account the sensitivity of the information that is being stored or processed by the cloud provider. These areas include:

- **Governance** – corporate policies, procedures and standards with respect to security and privacy.
- **Identity and Access Management** – controls surrounding access by cloud provider employees as well as employees and users of the public body's systems.
- **Infrastructure Security** – the management and ongoing maintenance of network, system and application security including layered security controls and patch management.
- **Encryption** – personal information should be encrypted during transmission between the public body and the cloud provider as well as in storage at the cloud provider's facilities to ensure that the information is not intercepted in transit and a breach of the cloud provider's systems does not result in the unauthorized disclosure of personal information.
- **Contractual provisions** – public bodies should address FIPPA in contracts with third parties. Contracts should include a requirement to notify the public body as soon as possible in the event of an actual or suspected breach of personal information. They should also include the right to conduct site visits and the ability to ask employees about the ways in which the third party is managing personal information on behalf of the public body. Contracts should also limit the right of the third party to use or disclose the personal information.[10]

For more information, see "Securing Personal Information: A Self-Assessment Tool for Organizations".[11]

---

[10] Public bodies should view these suggestions as a starting point only; they are not exhaustive. For more information, see the BC Government's information page on FIPPA and contracting, online at: www.cio.gov.bc.ca/cio/priv_leg/foippa/contracting/index.page.

[11] Although the Self-Assessment Tool applies to organizations and not to public bodies, the legal requirement to protect personal information is very similar. The Tool is a joint effort by the Office of

The Role of the Office of the Information and Privacy Commissioner

The Office of the Information and Privacy Commissioner is responsible for overseeing FIPPA. If an individual complains that a public body is improperly storing or accessing his or her personal information, the Commissioner may investigate. The Commissioner has the power under FIPPA to investigate a public body even if no one has complained. Following an investigation, the Commissioner could ask or order a public body to comply with FIPPA.

Conclusion

Public bodies in BC must consider FIPPA when making choices about whether to use cloud computing. While some organizations are offering cloud computing products that store personal information solely inside of Canada, public bodies should make appropriate inquiries to ensure that they can rely on the representations these organizations are making. No matter where a public body stores personal information, FIPPA requires public bodies to protect personal information. If public bodies choose to store personal information outside of Canada, they must only do so if FIPPA authorizes it.

If you have any questions about these guidelines, please contact:

Office of the Information and Privacy Commissioner for BC
Tel: (250) 387-5629 (in Vancouver call (604) 660-2421;
elsewhere in BC call 1-800-663-7867)
Email: info@oipc.bc.ca

Further Reading:

FIPPA:
The Act:
www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00
The Regulations:
www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/11_323_93

---

the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta, and this Office. It is available online at: www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1).

Office of the Information and Privacy Commissioner for BC:
Homepage: www.oipc.bc.ca
Text of speech by the Information and Privacy Commissioner on cloud computing:
www.oipc.bc.ca/pdfs/Speeches/FindingOurWayThroughTheClouds.pdf

The Office of the Privacy Commissioner of Canada:
Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing:
www.priv.gc.ca/resource/consultations/report_201105_e.cfm

Office of the Chief Information Officer
Ministry of Labour, Citizens' Services and Open Government:
Homepage: www.cio.gov.bc.ca
FIPPA information page: www.cio.gov.bc.ca/cio/priv_leg/foippa/index.page

Special Committee to review FIPPA:
Homepage: www.leg.bc.ca/foi
Report: www.leg.bc.ca/cmt/39thparl/session-2/foi/index.htm
Submissions received: www.leg.bc.ca/foi/submissions_received.htm

BCcampus
Ministry of Advanced Education:
Homepage: www.bccampus.ca/
Cloud computing information:
www.bccampus.ca/anonymizing-student-access-to-cloud-based-services/