Cloud computing, Social media, and Privacy

October 26, 2012

Bradley Weldon, Policy Analyst
Discussion topics

1. The role of the OIPC
2. FIPPA and PIPA
3. Cloud computing
4. Social media
5. Privacy Impact Assessments
Office of the Information and Privacy Commissioner

- Independent officer of the Legislature
- Regulator of public bodies and private sector organisations’ compliance with provincial privacy legislation
- Power to investigate and issue orders and public reports
Provincial privacy legislation

*Freedom of Information and Protection of Privacy Act (FIPPA)*

- privacy legislation that regulates the public sector
- requires that public bodies have legal authority for collection, use, and disclosure of personal information.
About FIPPA

- FIPPA applies to “public bodies”
- Each school district is a public body
- FIPPA limits the collection, use and disclosure of personal information
- The OIPC has oversight over FIPPA and can issue orders to ensure compliance
FIPPA regulation

Freedom of Information and Protection of Privacy Act

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY REGULATION

Definitions

1. In this regulation:
   "commercial applicant" means a person who makes a request for access to a record to obtain information for use in connection with a trade, business, profession or other venture for profit;
   "health professional" means a medical practitioner, psychologist, registered nurse or registered psychiatric nurse.

Oral requests

2. An applicant may make an oral request for access to a record if:
   (a) the applicant’s ability to read or write English is limited, or
   (b) the applicant has a physical disability that impairs his or her ability to make a written request.

Who may act for a minor

3. (1) A guardian of a minor may act for the minor in relation to any of the following sections of the Act if the minor is incapable of acting under that section:
   (a) section 5;
   (b) section 10 (1) (d);
   (c) section 26 (d);
   (d) section 27 (1) (a) (l);
   (e) section 29 (1);
   (f) section 30.1 (a);
   (g) section 32 (b);

Repositories:

B.C. Reg. 155/2012
O.C. 491/2012

Deposited June 25, 2012
FIPPA regulation

- describes the requirements for consent

** more on this later**
Provincial privacy legislation

*Personal Information Protection Act (PIPA)*

- privacy legislation that regulates the private sector
- consent-based; requires that organisations collect, use, and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances
What is personal information?
What is personal information?

"personal information" means recorded information about an identifiable individual

- Must be information “about” someone
- Can include descriptions of people
- Can appear in any format (email, photo, voice record)
- Includes unique numerical identifiers (student #)
- Public bodies have legal obligations for all the personal information in their custody or under their control
What is custody or control?

FIPPA and PIPA apply to public bodies or organisations that have custody or control of personal information.

- not defined in FIPPA or PIPA
- the meaning of custody or control is derived from caselaw and previous orders of the OIPC
- often just common-sense;
- do you have the ability to control access to the record?
- Is it in your possession?
So, you have custody or control of personal information...

Then FIPPA or PIPA apply, and you have responsibilities under those Acts regarding:

- accuracy and correctness of records
- responding to requests for access to records
- ensuring reasonable security arrangements for the personal information in your control

But what about cloud computing?
Cloud computing

Defined in several ways;
• software as a service
• platform as a service
• infrastructure as a service
The cloud is good?

Cloud services are attractive because they offer:

- Flexibility
- Low cost
- Reduced administrative burden
The cloud is bad?

FIPPA and the PATRIOT Act

• FIPPA was amended after the PATRIOT Act
• Cannot disclose personal information outside of Canada except in limited circumstances.
• Any disclosure outside of Canada must still comply with s. 30 requirement in FIPPA to protect against unauthorized access.
• Cannot disclose in response to foreign requests or demands
PATRIOT Act concerns

- information can be disclosed outside of Canada with consent

But...

- the public body must have the consent of all of the individuals with personal information on the record

- this can be challenging
Let’s just talk about servers

The cloud is distributed, but the data still resides on a server, somewhere...

The main FIPPA and PIPA issues are where is the data, and who has access?
FREQUENTLY ASKED QUESTIONS

Latest Revision: December 7th, 2010

Get to know Gmail

More Detail

Privacy

Less Detail

1. Has a Privacy Impact Assessment (PIA) on the potential risks of using Gmail been performed?
2. Does the PIA include all Google Apps for Education applications, or is it limited to only the email and calendar apps?
3. The PIA looks at the flow of data happening now, but would it be sustainable over 20 to 30 years?
4. Does the US Patriot Act allow the US government to access my personal information?
5. How does the US Government's ability to access my personal information differ from the Canadian Government's ability to do so?
6. Does the US Government have access to intelligence and personal information that has been collected by the Canadian Government?
Section 30 (FIPPA)
Section 34 (PIPA)

The biggest challenge in the cloud:

30 A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

34 An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.
Consent

FIPPA allows for consent to store personal information outside of Canada [s. 30.1(a)]

and,

for consent to disclose personal information outside of Canada [s. 33.1(b)]
Consent

• must be in writing;

• must specify to whom the personal information may be disclosed and how the personal information may be used;

• can be exercised on behalf of someone under 19 years old by a parent or guardian if they cannot exercise their right to consent.
  • this is contextual, but always safer to get parent to consent.
Consent Challenges

Public bodies must ensuring that the consent meets the requirements of the FIPPA regulation (s.11)

- All consents must:
  - be in writing; and
  - specify:
    - the personal information for which the individual is providing consent; and
    - the date consent is effective and, if applicable, the date consent expires.
Consent Challenges

Consent for storage outside of Canada must also specify:

- who may store or access the personal information;
- the jurisdiction in which the personal information may reside (if practicable); and
- the purpose of the storage of, or access to, the personal information.
Consent Challenges

Consent for **disclosure** outside of Canada must also specify:

- to whom the personal information may be disclosed;
- the jurisdiction in which the personal information may be stored (if practicable); and
- the purpose of the disclosure of the personal information
Great! So consent solves everything

But...

- Cannot consent out of the requirement to take reasonable security measures (s. 30/s.34)
- Many records contain more than one individual’s personal information
  - school project describing a family tree
  - short story about a summer vacation
- The consent provisions require that each individual must consent
Order F07–10 : Mission School District
OIPC Order F07–10

• School District used US based Gallup to provide an assessment tool job applicants were required to complete

• Gallup encrypted all data during transmission

• Gallup obtained consent from individuals before collecting personal information

• “In assessing the “reasonableness” of the security arrangements, consideration must be given to the nature of the personal information involved and the seriousness of the consequences of its unauthorized disclosure.” [72]

• “In the present case, I am satisfied that all of the personal information collected in the Assessment, with the exception of social insurance numbers, relates directly to the activity of recruiting and hiring teachers.” [32]
OIPC Order F07–10: Consent

- Commissioner determined that the consent was valid
- There was no evidence individuals were coerced to consent
- Electronic consent was valid
  - public body must later be able to establish that consent was given;
  - can be established by providing a process that cannot move beyond the consent page unless the individual consents.

- “It is critical to my finding that the consent form provides explicit notice to applicants that their personal information will be stored and accessed in the United States.” [89]
- “When a person consents to the transfer of his or her personal information to the United States, it necessarily follows that the information will be subject to the laws in force there”[100]
[85] I note in passing that, as indicated earlier, there will be cases where, in order to receive services or benefits from a public body, an individual is compelled to provide personal information or to permit it to be compiled. Many choices affecting one’s privacy are made on the basis of achieving a desired objective and this holds true in dealings with public bodies as with private sector organizations. One might prefer to choose not to provide government with, or permit it to compile, personal information that enables it to assess and collect income taxes that pay for public services, but that choice is not on offer.
Some other ways to disclose outside of Canada

• If it is authorized or required by law;
• or, for example, if it is temporarily necessary to troubleshoot or for data recovery after a system failure;
• or by Ministerial Order for a consistent purpose if it is necessary for performing the statutory duties of the public body.
The OIPC has issued guidelines on the use of cloud computing


Or

Search online for “cloud computing guidelines for public bodies”
Group Discussion
Canadians lead world in internet use: report

Canadians are the most active users of the internet in the world, according to a new global report.

Canadians spend an average of 43.5 hours online every month, according to ComScore, a firm that measures internet use and online trends. This is almost twice the global average of 23.1 hours.

Canada saw a two per cent increase in the total number of people online between 2009 and 2010. Much of this is attributed to significant growth in web use among people over 55 years of age, with a 4.2 per cent jump in new users recorded in that age group across the country over that period.

There was also a four per cent drop in internet usage among youths between the age of two and 17, but the report did not give any specific reasons for the change.

Social nation

The report shows that Canadians, particularly older individuals, are becoming more sociable in online spaces.

Visits to social networking sites saw a 13 per cent increase between 2009 and 2010, with seven per cent more people befriending others on Facebook. Twitter also saw 11 per cent more unique Canadian tweeters during that period.
How does FIPPA apply to social media?

First principles:

Public bodies need authorisation for:
• collection of personal information;
• storage of, or access to, personal information outside of Canada; and
• Disclosure of personal information outside of Canada;

PIPA organisations need consent
Collection

What authority do you have for collection of personal information from social media?

• may be necessary for the program or activity of the school/district, but viewing = collection
• It is likely that a school employee would “collect” personal information that is not necessary.
Assuming the social media site is hosted on servers outside of Canada;

When personal information is stored on a social media website, the school district may still have control of the information.

The same problem exists for social media as for cloud storage:
1. what authority do you have for storage of personal information outside of Canada?  
2. can you ensure that reasonable security measures are being taken to protect the personal information?
Disclosure can be complicated; assuming the social media site is hosted on servers outside of Canada;

What authority do you have for disclosure of personal information outside of Canada?

• Disclosure to the social media provider has occurred;
• have you reviewed its terms of service to determine what uses the information might be put to, such as targeted advertising?
Disclosure can be complicated; assuming the social media site is hosted on servers outside of Canada;

What authority do you have for disclosure of personal information outside of Canada?

If the school has “control” over the web page, then a student posting their own personal information on that page could be considered disclosure.
Disclosure

Disclosure can be complicated; assuming the social media site is hosted on servers outside of Canada;

What authority do you have for disclosure of personal information outside of Canada?

33.1 (1) A public body may disclose personal information inside or outside Canada as follows:

(r) if the information

(i) was disclosed on a social media site by the individual the information is about,

(ii) was obtained or compiled by the public body for the purpose of enabling the public body to engage individuals in public discussion or promotion respecting proposed or existing initiatives, policies, proposals, programs or activities of the public body or respecting legislation relating to the public body
Quick Legislative Update
FIPPA amendments

- Permits use of social media for public engagement and promotion
- Permits use of photos/video from public events
- Enables consent in certain instances
- Provides authority for the Ministry to direct public bodies to complete PIAs
- Must notify commissioner “at an early stage” of a data-linking initiatives or “common or integrated” programs
FIPPA Regulation amendments

- Came into force June 2012.
- Provides prescribed purposes for collection.
- Prescribed manner of consent.
- List of social media sites for disclosure outside of Canada [s. 33.1(r)]
Prescribed Social Media Sites
The following social media sites are prescribed for the purposes of the definition of "social media site" in Schedule 1 of the Act:

(a) Bebo;  (q) Gather;  (kk) PlaceSpeak;
(b) Blogger;  (r) Google+;  (ll) Posterous;
(c) blog.gov.bc.ca;  (s) GovLoop;
(d) Classmates;  (t) Gowalla;
(e) Couvon;  (u) Groupon;
(f) Dealfind;  (v) hi5;
(g) Delicious;  (w) Instagram;
(h) Diaspora;  (x) Kaboodle;
(i) Digg;  (y) Last.fm;
(j) Elluminate;  (z) LinkedIn;
(k) ethicalDeal;  (aa) LiveJournal;
(l) Eventbrite;  (bb) LivingSocial;
(m) Fark;  (cc) Meetup;
(n) Flickr;  (dd) Metacafe;
(o) Fotki;  (ee) Movable Type;
(p) foursquare;  (ff) Ning;
  (gg) orkut;
  (hh) Photobucket;
  (ii) Picasa;
  (jj) Pinterest;
  (kk) PlaceSpeak;
  (ll) Posterous;
  (mm) Prezi;
  (nn) reddit;
  (oo) Scribd;
  (pp) SlideShare;
  (qq) SoundCloud;
  (rr) StumbleUpon;
  (ss) SwarmJam;
  (tt) Tagged;
  (uu) TeamBuy.ca;
  (vv) Tumblr;
  (ww) Typepad;
  (xx) Vimeo;
  (yy) WagJag;
  (zz) Windows Live;
  (aaa) WordPress;
  (bbb) Yammer;
  (ccc) Yelp;
  (ddd) Zoomr.
Some questions

1. Can schools interact with parents and students using Facebook?
   • if disclosed by the individual the info is about;
   • was obtained for the purpose of engaging individuals in public discussion or promotion of programs; and
   • was disclosed for that purpose.
2. What if students already have accounts?

- if the school has control of the page/website then the information is likely being disclosed by the school, regardless of how the students access the service.
Some questions

3. Are schools responsible if employees use a cloud service in a manner that is not compliant with FIPPA or PIPA?

• if the employee is acting in the course of his or her duties then the public body is likely responsible.
• School districts should have policies in place to address these issues, and should ensure that employees understand the policies.
Some questions

4. Can schools publish photos/videos from public events such as a football game or band performance?

- FIPPA allows this type of disclosure if:
  - the individual in the photo or video voluntarily attended; and
  - the event was open to the public
Thank you.
Bradley Weldon, Policy Analyst
www.oipc.bc.ca