The cloud thing: Privacy and cloud computing

David T.S. Fraser (david.fraser@mcinnescooper.com / @privacylawyer)
University of New Brunswick
July 2011
What follows are the views of the author and are not legal advice.

This is a complicated area of law that puts obligations (sometimes very different obligations) on the universities and on the service providers.
What is “cloud computing”

- Distributed computing architecture in which data and applications reside on servers separate from the user and are accessed via the internet. Applications and data are generally accessible from anywhere, provided you have a net connection.
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.
NIST Characteristics

- On-demand self-service.
- Broad network access.
- Resource pooling.
- Rapid elasticity.
- Measured Service.
Why cloud computing?

- **Low cost of administration** – providers are able to adopt economies of scale
- **Scalable** – can easily deploy the service to a flexible range of users
- **Greener** – large data centres are located near green energy, harness efficiencies that single-customer data centres cannot
Back to the beginning?

Timeshared Mainframes

Personal Computers

Corporate mainframes
Dumb terminals
Smarter terminals
Personal computers
Portable computing
Portable computing
Portable computing
Cloud-only computing

Chromebook
Nothing but the web
The end of an era

- The desktop computing era is over.
- Welcome to the “ubiquitous computing” era.
Examples

• Free or mass-market services:
  – GMail, Hotmail, Yahoo! Mail
  – Google Documents, MS Office Online
  – Hosted exchange servers, telephony

• Social media services
  – Facebook, Flickr

• Niche services:
  – Salesforce.com
  – Photoshop.com
Your cloud life?

On your PC
- MS Outlook
- MS Office – Word
- Office – Excel
- MS Project
- Photoshop
- Instant Messaging

In the cloud
- Gmail/Hotmail
- Google Documents / Office 365
- Google Spreadsheets / Office 365
- Basecamp
- Photoshop.com
- Google Talk / Communicator
Privacy issues

• Principal issue is that information is no longer in your direct custody or control.
• You no longer directly secure your data.
• Information is handed over to a third party to manage
• Information may be resident in a different jurisdiction or multiple jurisdictions
• Mass-market cloud services are subject to “take it or leave it” service agreements
• Information and data may not be “portable” – you can’t take it with you
Privacy benefits

- Professional management
  - More secure data centres
  - More resources for security
  - Better auditability
- Data is not easily lost
  - Laptops
  - Thumb drives
  - Portable hard-drives
Is cloud computing forbidden due to privacy issues?

Often not, as these can be managed

Maintain accountability and ensure security
Managing privacy issues

• Don’t entrust personal information to “take it or leave it” service agreements
• Under PIPEDA, the original custodian remains responsible for personal information
• You cannot outsource or delegate responsibility

“4.1.3

An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party”
• How important is jurisdiction?
• Where will the data be?
• Perhaps not the roadblock you’ve been led to believe
• Except in some provinces
  – Nova Scotia
  – British Columbia
  – Alberta
USA Patriot Act

- National Security Letters
- Roving Surveillance
- *Foreign Intelligence Surveillance Act* Court – “Secret court, with secret hearings, issuing secret order.”
  - FISA Court Orders to produce “any tangible thing”
- USA Patriot Act generally extends existing US national security laws
Issue for Canadians

- The *USA Patriot Act* expands law enforcement’s surveillance and investigative powers.
- New powers of surveillance and search/seizure extend to records of anyone (including Canadians) in the US.
Basis of jurisdiction

• Generally, governments can take jurisdiction over anything or anyone within their borders
  – Data in the jurisdiction
  – Data manager in the jurisdiction
  – Someone who can access the data in the jurisdiction
  – Also, citizenship
Arguably, new powers extend to
- Records in the US
- Records in the custody of
  - US companies in Canada
  - Canadian subsidiaries of US companies
  - Canadian companies with presence in US

Issue for Canadians
First vocal response came from the British Columbia Government Employees Union (BCGEU)

Against outsourcing of medicare processing to Maximus (American IT service provider)

BCGEU launched its “Right To Privacy Campaign” – May 10, 2004
BCGEU Campaign

I want you

US federal authorities have the right access to your confidential financial information, including your Social Security numbers, credit history, fingerprints, even your medical records.

That’s because the Carnegie Corporation are contracting out the administration of Personal Information to the government with national corporations, making your personal identity and financial records subject to review by people with no security clearance.

B.C. Government and Health Services Employees’ Union

www.bcg.eu.ca

McInnes Cooper

Atlantic Canada’s Law Firm

New Brunswick  Newfoundland & Labrador  Nova Scotia  Prince Edward Island  mcinnescooper.com
Don't Care Card

Premier Campbell wants to sell off the services that make Medicare work

By privitizing critical health care services like our health services plan and PharmaCare is a bad decision. By today's globalization reality the only real benefit will go to large corporations like the Campbell government will do to privatize this important and valuable service.

It won't work

The multinational companies who run these multinational corporations are not interested in improving conditions. Instead they are interested in making a profit and were less interested to provide quality care. This has been shown in a lot of cases.

The American government has itself a lot of problems and face a lot of challenges with our health care. The American government has itself examples of overcharged, failed to deliver services, and improper billing.

It failed in the US

The state of Connecticut regulates a setting or else from companies handling Medicare claims. This has been found to be criticized for high rates of improper billing and policy decisions that don't benefit the state of Connecticut.

Gordon Campbell's privatization plan is a threat to your privacy and to B.C.'s health care system.

Don't sell off the Medical Services Plan or PharmaCare

Sign the petition at: www.petitiononline.com/publicpcp
Should your private medical records be given to American corporations?

Please help stop Campbell from selling off MSP and Pharmacare

The Gordon Campbell Liberal plan to sell off the Medical Services Plan and Pharmacare to the American multinational corporations - by August 31. The government will give an American-owned corporation access to private records on every B.C. resident. This includes health treatment, pharmacy income tax, mental health and criminal records, as well as records from the ministries of Children and Family Development and Human Resources.

A New York expert on the new USA Patriot Act says this could even give the FBI access to our private medical records and leave us vulnerable to other personal information of innocent people. And U.S. legal precedents suggest even if the information is held by a Canadian subsidiary, the American parent company would be required to hand it over.

Our personal medical information should not be made available to private corporations that don't answer to our privacy laws. It should remain in the care of public employees who are bound by an oath of office to keep it confidential.

For more information, and to sign the petition, visit www.bcgceu.ca/1719

B.C. Government and Service Employees Union

Atlantic Canada's Law Firm

New Brunswick  Newfoundland & Labrador  Nova Scotia  Prince Edward Island  mcinnescooper.com
Information and Privacy Commissioner of BC began an inquiry into the *USA Patriot Act* and British Columbians’ privacy – Spring 2004

- Particularly focused on s. 215 – secret court orders allowing seizure of “any tangible thing”.
- Received over 500 submissions, including from the FBI and Maximus.
Before final Commissioner report, BC government introduced amendments to the *Freedom of Information and Protection of Privacy Act*.

- Passed on October 19, 2004.
- Wide prohibition against disclosures outside of Canada.
Alberta amendments

- Does not directly affect the University
- Affects the service provider

- Service provider probably cannot comply in reality: If the information is subject to a US demand for disclosure, Alberta statute will not trump the US statute.
- Some service providers may see the risk of having to actually deal with this as remote.
Freedom of Information and Protection of Privacy Act

92(3) A person must not wilfully disclose personal information to which this Act applies pursuant to a subpoena, warrant or order issued or made by a court, person or body having no jurisdiction in Alberta to compel the production of information or pursuant to a rule of court that is not binding in Alberta.

(4) A person who contravenes subsection (3) is guilty of an offence and liable

(a) in the case of an individual, to a fine of not less than $2000 and not more than $10 000, and

(b) in the case of any other person, to a fine of not less than $200 000 and not more than $500 000.
Nova Scotia Response

- Obligations on the University and on the service provider
- Limitations on exports and prohibitions against disclosures pursuant to a foreign demand for disclosure
- Service provider probably cannot comply in reality: If the information is subject to a US demand for disclosure, NS statute will not trump the US statute.
- Some service providers may see the risk of having to actually deal with this as remote.
• **Personal Information International Disclosure Protection Act**

• **General rule:**
  - Personal information must be stored in Canada and accessed only from Canada

• **Exceptions:**
  - Consent of the individual in the prescribed form
  - Permitted disclosure under the Act
  - Storage or access permitted by head of the public body
Nova Scotia’s PIIDPA

• Exception:
  – Head of the public body can permit storage or access outside of Canada if the head considers the storage or access is to meet the necessary requirements of the public body's operation
  – Head can impose restrictions and conditions
  – Head must report all such decisions to the Minister within 90 days of the end of the relevant year
Public body that is a law enforcement agency may disclose personal information to:

(a) another law enforcement agency in Canada; or
(b) a law enforcement agency in a foreign country under an arrangement, a written agreement, a treaty or an enactment of the Province, the Government of Canada or the Parliament of Canada.
9(4) The head of a public body may allow a director, officer or employee of the public body to transport personal information outside Canada temporarily if the head considers it is necessary for the performance of the duties of the director, officer or employee to transport the information in a computer, a cell phone or another mobile electronic device.
New Brunswick

• Has not passed any equivalent of the BC, Alberta or Nova Scotia provisions.

• Universities are subject to the Right to Information and Protection of Privacy Act
Using cloud services in an university has been challenged by arbitration in the Lakehead case: *Lakehead University (Board of Governors) v. Lakehead University Faculty Association*, 2009 CanLII 24632 (ON L.A.)

Arbitrator found it was not contrary to the collective agreement and faculty members were not required to use the service.
Canadian National Security
Access to Personal Information
Anti-terrorism Act – passed by parliament and became law on December 24, 2001.

Amended a range of statutes, including

- Criminal Code
- Canadian Security Intelligence Service Act
- National Defence Act
Canada – interception of e-mail

- Interception of e-mail *in transit* would require a wiretap order under the *Criminal Code*, *CSIS Act* or ministerial authorization under the *National Defence Act*.

- Access to an e-mail in storage would require a search warrant or production order under the *Criminal Code* or order under the *CSIS Act*.
Canada – CSIS Act

- Allows secret orders from secret court (Specially designated judges from the Federal Court)
- Allows a secret warrant authorizing
  - Interception of communication
  - Obtaining any information, record, document or thing
- Can obtain these by
  - Entering any place
  - Searching, removing and examining any thing
  - To install, maintain or remove any thing.
Provisions added by *Anti-terrorism Act* refer to the Communications Security Establishment (the Canadian NSA)

Minister (not court) can authorize interception, for the purpose *foreign intelligence*, of private communications directed at foreign entities located outside of Canada.

Note: “foreign intelligence” means information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or *terrorist group*, as they relate to international affairs, defence or security.
Information sharing

- Canadian and US intelligence agencies share vast amounts of information
- Mutual legal assistance treaties allow Canadian authorities to get warrants for US authorities, and vice versa
- “Arrangements” exist for informal sharing related to targets of mutual interest
- Canadian authorities can get information in the US without a warrant and American authorities can get information in Canada without a warrant
USA Patriot Act – myth v reality

• **Reality**: Most of the provisions of the USA Patriot Act are mirrored in Canadian law

• **Reality**: Canada has a “secret court” that allows *ex parte* applications for warrants, including sneak and peek warrants

• **Reality**: Canada has warrantless wiretap powers for international communications, same as in the US

• **Reality**: There is a huge degree of cooperation between Canadian and US authorities, both formal and informal
Getting back to first principles

• The original custodian remains responsible for protecting and safeguarding the personal information

• The original custodian needs to make informed choices about how to handle the data, including what services and service providers to use for its processing

• Should be a risk-based approach
  – What is the sensitivity of the information?
  – What is the risk to the data?
  – What role does the jurisdiction play in that risk?

• If the risk is high and the safeguards cannot be assured, then don’t use the service provider
Service provider contracts

Wish list:

1. Limit service provider to only using your data for your purposes and for no other purpose
2. Include provision that data is held “in trust” for customer
3. No disclosures of information without your consent
4. Obligation to resist – to the extent lawful – orders to disclose information without consent
5. Liquidated damages for any disclosure without consent
6. Obligation to cooperate with you in any regulators’ investigations
7. Will not deal with any regulators related to your information without your participation
8. Implement safeguards to protect information – Set minimums but shift as much responsibility to the service provider
9. Do not accept any limitations of liability related to privacy and security – full indemnity
10. No retention of your information
Additional concepts

• The service provider is generally not a public body to which RIPPA applies

• Service provider is an agent of the public body
  – But … some statutes push obligations down to service providers
Additional concepts

• Consider whether RIPPA applies at all to portions of the service
• Does RIPPA actually apply to student e-mail and student documents?
• Is it under the control of the institution?
• If not, RIPPA probably doesn’t apply to such services if outsourced.
• (Administration and instructional materials are almost certainly under the control of the institution.)
Some online providers have been over-reaching in the licenses they seek through the terms of service

- Facebook – reversed after backlash
- Twitpic – backlash in progress

- broad rights to license, sublicense and otherwise use uploaded images, whether for commercial purposes or not and whether compensated or not, without any obligation to pay anything to the content owners.
A note about copyright

- CAUT sometimes cites the following from Google’s Educational Terms of Service:

  6.1 **Intellectual Property Rights.** Except as expressly set forth herein, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other’s intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer Data, and Google owns all Intellectual Property Rights in the Services.

- These TOS have zero impact on staff/student ownership of intellectual property rights.
- Does not affect ownership one iota.
- University needs to examine terms and be cautious, but it generally is not a real issue.
Questions? Discussion?
David is the chair of McInnes Cooper's Privacy Practice Group, working with large and small clients to implement compliance programs for Canadian privacy laws. He regularly provides opinions related to Canadian privacy law and is a frequently invited speaker on this topic. David also acts for organizations in addressing complaints to the Privacy Commissioner.

David is the past President of the Canadian IT Law Association and former Chair of the National Privacy and Access Law Section of the Canadian Bar Association. He has appeared before the Standing Committee on Access to Information, Privacy and Ethics of the Canadian Parliament and has contributed to the CBA's submissions on privacy law reform, criminal justice matters, submissions to the Arar Inquiry, the Air India Inquiry, to name a few.

David was honoured to be included in the inaugural (2006) edition of The Best Lawyers in Canada in the category of Information Technology law. In the spring of 2006, David was a recipient of an Outstanding Young Canadian Award by the Junior Chamber of Commerce International - Halifax Chapter. The JCI's Outstanding Young Canadians Award Program recognizes outstanding individuals between the ages of 18 and 40 who exemplify the best attributes of the world's young people.