Privacy and cloud computing

David T.S. Fraser (david.fraser@mcinnescooper.com)

Cloudlaw.ca

October 14, 2011

Disclaimer

- Opinions are personal and should not be attributed to McInnes Cooper or its clients.

Privacy issues

- Principal issue is that information is no longer in your direct custody or control.
- 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

Security

- Most people have an unrealistic understanding of their current security situation
- PARTICULARLY when looking at cloud computing as an option
- Assume that their current situation is ok

Privacy benefits

- Professional management
  - **More secure data centres** - No small or medium size enterprise in Canada can afford to operate a Tier 4 data center
  - **More resources for security** - No company in Canada has the number of security professionals as the major cloud vendors.
  - **Better auditability** - You have no idea what is being done and by whom with data that it off your systems.
- Data is not easily lost

Privacy issues

- 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"

Jurisdiction

- How important is jurisdiction?
- Where will the data be?
- Perhaps not the roadblock many believe
- Except in some provinces
  - Nova Scotia
  - British Columbia
  - *Alberta*

USA Patriot Act

- National Security Letters
  - Administrative subpoenas for non-content information, signed by senior Justice Department officials
- *Foreign Intelligence Surveillance Act* Court – "Secret court, with secret hearings, issuing secret order."
  - FISA Court Orders to produce "any tangible thing"
- Usually coupled with a gag order

Issue for Canadians

- The *USA Patriot Act* expands law enforcement's surveillance and investigative powers
- Anybody with a US presence is affected by it
- Arguably, powers extend to records in the custody of
  - US companies in Canada
  - Canadian subsidiaries of US companies
  - Canadian companies with presence in US

Canadian Response

- 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

BCGEU Campaign

BCGEU Campaign

BC Commissioner's Inquiry

- 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.

BC FOIPPA Amendments

- 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 public body
- 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.

Alberta amendments

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 public body 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.

Nova Scotia Response

- *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

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

S. 9(3) – Law Enforcement

- Very ironic
- 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.

Canadian National Security Access to Personal Information

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 - Anti-terrorism Act

- *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 – *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.

Canada – *National Defence Act*

- 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

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

Questions? Discussion?

MCINNES COOPER

LAWYERS | AVOCATS

Atlantic Canada's Law Firm

New Brunswick Newfoundland & Labrador Nova Scotia Prince Edward Island mcinnescooper.com