Cloud Privacy for the Public Sector

Issues and Considerations

Alec Campbell
Excela Associates Inc.

Leanne Salel
Office of the Information and Privacy Commissioner of Alberta

IAPP Canada Symposium, May 2015

Introduction

- OBJECTIVES
  - Highlight differences between public sector and private sector organizations in cloud computing privacy issues
  - Focus attention and stimulate discussion on the protection of privacy in public sector cloud computing arrangements, to the extent that it may differ from the private sector.

Issue: Consent

- Major public-private sector differentiator
- Public: authority for PI collection is mostly legal authority, not consent
  - Where PI collected without consent, organization has a greater responsibility to protect that information
- Private: authority for collection mostly from consent

Issue: Choice

- Private sector clients usually have choice of provider
  - Except monopolies
- Public sector clients usually do not
  - e.g. healthcare, services for disadvantaged, regulatory services, law enforcement
  - Except certain publicly-owned entities with market competition
- Greater obligation to protect PI when no choice of provider

Issue: Location of Data

- In Canada:
  - Subject to Canadian law
  - General consistency in legislation across Canada
  - Subject to authority of Canadian regulators
- Outside Canada
  - Not subject to Canadian law
  - Must rely exclusively on contractual enforcement
  - Regulators have limited authority
- Larger issue for public sector
  - Per contractual, consent, choice, accountability issues

Issue: Contracts

- Contract is paramount in cloud services
  - especially if data outside Canada & Canadian law doesn't apply
- Most standard cloud contracts have private sector in mind
- Public sector organizations often have less flexibility
  - Govt open competition requirements
  - Public sector budget inflexibility
  - Public sector need to address policy issues
- Standard contracts often insufficient for public sector

Issue: Security

- Cloud security often best of breed
- But security specifics may not be available to clients
  - Problem for due diligence
  - Due diligence larger issue for public sector
- Accessibility of audit and investigation info
  - Investigators (for clients and regulators)
  - Contractual enforcement
- Breach notification requirements
- “Zero-knowledge” encryption of data at rest

Legislation and Policy

- Legislative differences
  - BC, NS public sector: no PI outside Canada
  - AB private sector: inform individuals if PI outside Canada
  - AB healthcare: agreement if data outside Canada
  - QC, AB private sector: no disclosure to court without jurisdiction
- PIPEDA accountability, transparency principles
- Public sector legislation often supplemented by prescriptive policy – not always so in private sector

Accountability

- Accountability differences
  - Private sector accountable to shareholders
  - Public sector accountable to all residents, via govt
  - Healthcare accountable to patients and professions
- Public sector policy requirements give effect to accountability
  - e.g., PIA requirements in both legislation and policy
- Ethical duty of due diligence in public sector

Health Care

- Special public/private sector case
  - Extreme sensitivity of PHI
  - Sectoral legislation with privacy requirements
  - Electronic medical records and EHRs (often cloud services)
  - Very wide internal organizational access to PHI
  - Excellent source of PI for identity theft, especially when privately billed
- Large number of breaches (per media reports)
  - Mostly by insiders in Canada
  - Mostly by hackers in the USA

Health Care Cont'd

- Data matching
  - Academic, clinical, epidemiological research
  - Operational research, e.g., to detect billing fraud
  - A privacy issue despite ethics boards due to absence of consent
- All of the above can be exacerbated by cloud computing involving PHI

Public Sector: High Risk Scenarios

- Sensitive PI (i.e., clinical health information) or confidential 3rd party business information to be stored/processed
- Public body's clients have little or no choice of service options and/or no notice re cloud services
- Vendor will not negotiate custom contract
- Data storage not restricted to Canada and not encrypted with private keys
- Vendor security, privacy measures inadequate, unclear not binding.

Public Sector: Low Risk Scenarios

- Less sensitive PI to be processed/stored
- Public body's clients have some choice of service options and/or are given notice re cloud services
- Vendor willing to engage in some customization of contracts
- Vendor offers storage in Canada, including backup and disaster recovery locations.
- Robust vendor security/privacy measures which are transparent to the public body.

What can the Public Sector Do?

- Pooling contracts for larger contractual influence
  - e.g., province-wide contracts for GAFE & similar services?
- Cloud-specific policies and strategies
  - e.g., Treasury Board Secretariat RFI of 2014
- Certification/ accreditation of cloud services to privacy & security standards
  - e.g., USA FedRAMP (www.fedramp.gov)
- Encouragement of Canadian hosting solutions

What can Cloud Providers Do?

- Recognize international variation in privacy requirements
  - Offer Canadian hosting
  - Be willing to provide some customization of contracts or contract schedules
- Provide pro-active content for privacy impact assessments
- Provide well designed, effective PbD features
  - demonstrable (more than lip service)
  - consistent with privacy principles and legislation
- Provide “zero-knowledge” encryption of data at rest

Additional Resources

- *Cloud Computing Guidelines for Public Bodies*, BC OIPC
- *Industry Cloud Computing Consultation RFI*, Treasury Board Secretariat
- *Guidelines on Security and Privacy in Public Cloud Computing*, NIST, US Department of Commerce
- *Taking Privacy into Account Before Making Contracting Decisions*, Treasury Board Secretariat

We're done!

Questions, comments, concerns?

Leanne Salel
Office of the Information and Privacy Commissioner of Alberta
lsalel@oipc.ab.ca

Alec Campbell
Excela Associates Inc.
alec@excela.ca